US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/31/2024

OPDIV:

NIH

Name:

United NCATS Authentication (UNA)

PIA Unique Identifier:

P-2151616-735616

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

Unified National Center for Advancing Translational Sciences (NCATS) Authentication (NCATS UNA) is an identity brokering hub service provider that establishes trust relationships with other identity management systems (NIH Identity, Credential, and Access Management (IAM) Services, HHS Personal Identity Verification (PIV), Login.gov, In-Commons Federated, etc.) to allow NCATS internal and external users to validate their credentials with the issuing identification (ID) Provider before gaining access to NCATS' information technology (IT) resources. NCAT UNA facilitates secure collaboration between researchers from diverse institutions and business partners.

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

NCATS UNA collects name, email address, organization, device identifiers, and information shared by the authorized Identity Providers (IdPs) (job title, roles or group association, and/or memberships)

Those requiring access to this system log in using the NIH IAM Services which maintains its own unique privacy impact assessment (PIA) on record, with 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 collects unique user credentials and stores them in an encrypted format. The IAM Service is an essential service which facilitates and governs network access to various resources.

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

NCATS UNA is an identity brokering service for identity providers management systems including NIH IAM, HHS PIV, In-Common Federation and Login.gov. NCAT UNA facilitates secure collaboration between researchers from diverse institutions and business partners.

NCATS UNA collects name, email address, organization, and device identifiers. Information shared by authorized IdPs with established trust relationships can include job title, roles or group association, or memberships.

Those requiring access to this system log in using the NIH IAM Services which maintains its own unique privacy impact assessment (PIA) on record, with 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.

Name
E-Mail Address
Device Identifiers
Organization, job title, roles or group association, memberships

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?

10,000-49,999

For what primary purpose is the PII used?

Personally identifiable information (PII) is required to verify individual as an authorized users and grant access to specific NCATS resources.

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.

5 USC 301, Departmental Regulations,

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.

09-25-0216 Administration: NIH Electronic Directory

09-90-0777, Facility adn Resource Access Control Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the DOI

Other HHS Operating Divisions

Non-Government Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Pub. L. 104-191, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

Is the PII shared with other organizations?

No

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

A consent statement is published in the privacy statement. The Consent statement addresses the essential information required for access to NCATS resources.

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 method for individuals to opt out. The information is voluntary and necessary for the purpose of granting access to NCATS resources. If the individual's identity provider does not share this information, authorization to NCATS resources is not allowed.

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

Changes to our policy will be posted on the privacy page so that NCATS collaborators and partners are always aware of what information we collect, how we use it and under what circumstances we disclose it.

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.

A generic email address (NCATSAuthSupport@mail.nih.gov) is available on the site's privacy statement to resolve individual's concerns.

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

NCATS will conduct an annual review of PIA to ensure the integrity, accuracy and relevancy of the data.

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 level and permission to PII is based upon job responsibilities and a need-to-know basis. An NIH IAM Services account is required to gain access.

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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users minimum access to 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. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). Training is completed on the https://irtsectraining.nih.gov site with valid NIH credentials.

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

NCATS direct contractors have completed the NIH Role-based training for IT System 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.

Records are retained and disposed of under the authority of the NIH Records Retention Schedule.

07-210 Public Key Infrastructure (PKI) administrative records. Other (non-Federal Bridge Certification Authority (FBCA)).
Records are PKI-unique administrative records that establish or support authentication by tying the user to a valid electronic credential and other administrative non-PKI records that are retained to attest to the reliability of the PKI transaction process.
Disposition: Destroy/delete when 7 years 6 months to 20 years 6 months old, based on the maximum level of operation of the Certification Authority (CA), or when no longer needed for business, whichever is later.

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

Administrative Control - NCATS Administrators and personnel who access IT systems have met the required NIH background investigation criteria. All personnel have completed the mandatory security and privacy training classes and the annual refreshers. Administrative and IT personnel use a separate privileged account for administrative access to this system.

Technical Controls: All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain the integrity of data. Sensitive and PII data is encrypted at rest and in transit.

Physical Controls: The NCATS UNA resides in the NCATS Data Center where policies and procedures are in place to restrict access to the facility and systems. This includes authorized access granted through Datawatch key fob system.