US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/12/2025

OPDIV:

NIH

Name:

NIAAA Azure Cloud

PIA Unique Identifier:

P-6012531-966929

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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?

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.

The National Institute on Alcohol Abuse and Alcoholism (NIAAA) Azure Cloud is a Microsoft Azure Cloud environment hosting internal NIAAA web applications, currently including the NIAAA Pay Plan System (NPPS) and the LabShare Authentication (LSAuth) application.

The NPPS application is tailored to NIAAA’s specific budgeting processes which automates data downloads, curation, and ingestion from the NIH Information for Management Planning Analysis and Coordination (IMPAC) II (including the Query/View/Reporting System (QVR)) and uploads funding decisions to NIH eRA Commons, the NIH system of record.

The LSAuth application acts as a Security Assertion Markup Language (SAML) broker, which is a custom federated authentication broker to NIH login for NIH employees and direct contractors

eRA is not an acronym

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

The NIAAA Azure Cloud hosted applications include NPPS and LSAuth.

NPPS collects, maintains and/or shares name, email and NIAAA grants information (needed to manage ranking, schedule reviews, and manage approvals in coordination with NIAAA administrative staff, division directors, and budget analysts).

Grants information is ingested from the NIH IMPAC II (including QVR) system, a module/application within eRA. Funding decisions are then uploaded (shared) to the eRA system. eRA is the system of record for grants data and maintains its own unique privacy impact assessments (PIA).

LSAuth does not collect, maintain, or share personally identifiable information (PII).

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique 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.

The NIAAA Azure Cloud is a Microsoft Azure Cloud environment hosting internal NIAAA web applications, currently including the NPPS and the LSAuth applications.

The NPPS application is tailored to NIAAA's specific budgeting processes which automates data downloads, curation, and ingestion from the NIH IMPAC II (including QVR) and uploads funding decisions to NIH eRA, the NIH system of record. NPPS collects, maintains and/or shares name, email and NIAAA grants information (needed to manage ranking, schedule reviews, and manage approvals in coordination with NIAAA administrative staff, division directors, and budget analysts).

The LSAuth application acts as a SAML broker, which is a custom federated authentication broker to NIH login for NIH employees and direct contractors. LSAuth does not collect, maintain, or share PII.

Grants information is ingested from the NIH IMPAC II (including QVR) system, a module/application within eRA. Funding decisions are then uploaded (shared) to the eRA system. eRA is the system of record for grants data and maintains its own unique PIA.

Those requiring access to this system log in using the NIH IAM Services which maintains its own unique 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
NIH grant financial information

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

Public Citizens

NIAAA Grantees (or potential grantees)

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

NIH grant funding information approval workflow notifications and reporting of grant funding statuses.

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.

The legal authority to collect information and maintain this system is: 5.U.S.C. 301; 42 U.S.C. 217a, 241, 242, 281, 282, 284, 284a, 285, 285b, 285c, 285d, 285e, 285f, 285g, 285h, 285i, 285j, 285k, 285l, 285m, 285n, 285o, 285p, 285q, 285r, 285s, 285t, 286, 287, 287b, 287c-11, 287c-21, 287d, 288, 44 U.S.C. 3101, 35 U.S.C. 200-212, 48 CFR Subpart 15.3, and 37 CFR 401.1-16;

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

N/A

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.

The Privacy Notice and disclaimers are posted on the eRA commons login page.

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.

Collection of PII is required and there is no option to opt out, although submission is voluntary.

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

A Privacy Act Statement warning banner is posted on the eRA Commons website, but there is not a specific process to notify individuals and obtain consent from individuals when major changes occur

to the system. Grants information which contains the PII is ingested from the NIH IMPAC II (including QVR) system. Funding decisions are then uploaded to the eRA system. PII is provided by NIAAA grantees (and potential grantees) voluntarily.

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 their Privacy Coordinator or the NIH Senior Official for Privacy 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.

PIA's are conducted prior to any new application being added to the NIAAA Azure Cloud environment and are reviewed on an annual basis as part of the NIH Security Authorization and Assessment process. In addition, anything privacy related is reviewed as part of the normal change management process.

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.

Determinations are made based on role-based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

Access to PII is assigned to personnel based upon current job responsibilities. An IAM account login is required to gain access to the stored PII data.

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.

NPPS application users have access limited to the minimum information necessary to perform their specific role within the application.

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.

In accordance with NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security and privacy 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).

The HHS Role-Based Training Course " IT Administrator Training" and "NLM Application Security Checklist & Best Practices for Developers" is required for all privileged access.

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.

Item 02-005: Official Case Files of Applications and Awards, Appeals, and Litigation Records for Grants, Cooperative Agreements, and Other Transaction Activities.

Description: Official case files of funded and unfunded grants and cooperative agreements, award

applications, and appeals and litigation records. Records also include those supporting other transaction awards and activities. These records include, but are not limited to, the complete application(s), summary of review actions, award notices, progress reports, financial records, audit records, official correspondence, appeal documents, legal opinions and litigation documents, closeout documents, and all other related significant and supporting documents that pertain only to the particular grant and grant owner(s). This schedule allows for all records in a case file that are stored in the same system to co-mingle.

Disposition: 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 proceedings concluded). Destroy 30 year(s) after cutoff. Disposition Authority: DAA-0443-2019-0008-0001

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

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Physical Controls: all computing infrastructure (e.g. Servers) housing PII are required to be maintained within an AWS GovCloud data center that has controlled access that is compliant with Federal Risk and Authorization Management Program (FedRAMP) for cloud service offerings.