US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/28/2025

OPDIV:

NIH

Name:

NIDA IRP Network

PIA Unique Identifier:

P-9067023-448062

The subject of this PIA is which of the following?

General Support System (GSS)

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?

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

No

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

PIA Validation

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

This validation is intended to refresh content and detail the type of personally identifiable information (PII) the general support system could maintain through the child systems.

Describe the purpose of the system.

The National Institute on Drug Abuse (NIDA) Intramural Research Program's (IRP) General Support System (GSS) is a General Support System (GSS) which provides physical infrastructure that supports various applications and services in support NIDA IRP’s mission. It also provides office automation and information processing services to NIDA research and management programs.

Applications residing on the GSS can collect and store sensitive information or PII from NIH Enterprise source systems (NIH Employee Directory (NED), NIH eRA). These systems include:
Animal Care and Research Solutions (ACRS)
Scientific Computing and Informatics Core Collaboration and Scheduling System (SCIC CSS)

Health Outcome of Neighborhoods (HONet)
Human Research Information System (HuRIS)

Each system maintains their own individual Privacy Impact Assessment (PIA) with all legal authorities documented and lists the NIDA IRP GSS's Universally Unique Identifier (UUID) within their individually maintained PIAs.

The GSS serves as an expedient repository for personally identifiable information (PII) within its network/data storage purposed for individual or group network drive assignments.

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

The NIDA IRP GSS is comprised of numerous services such as security appliances, security tools, software life cycle management tools, networking devices, enterprise storage solutions, application hosting resources, and enterprise communications services.

This GSS provides access to applications and services, such as basic office automation capabilities, specialized commercial off-the-shelf software supporting management and research functions and custom applications serving both the Institute's core business areas and administrative support for standalone, networked, and remote users.

Data from the enterprise (source) systems are stored on select network file shares and can include Social Security Number, Name, Date of Birth, E-Mail Address, Phone Numbers, Education Records, Mailing Address, Employment Status, Mother's Maiden Name, Medical Records Number, Medical Notes, Photographic Identifiers.

Data, at rest and in transit between these systems and the GSS infrastructure is encrypted and follow strict Federal Information Processing Standards (FIPS).

Users requiring access log in using NIH Identity and Access Management Services (IAM) which maintains its own 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 collect unique user credentials and store them in an encrypted format. The IAM Services are 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 NIDA IRP GSS is comprised of numerous services such as security appliances, security tools, software life cycle management tools, networking devices, enterprise storage solutions, application hosting resources, enterprise communications services. This GSS provides access to applications and services, such as basic office automation capabilities, specialized commercial off-the-shelf software supporting management and research functions and custom applications serving both the Institute's core business areas and administrative support for standalone, networked, and remote users.

Applications residing on the GSS can collect and store sensitive information or PII from NIH Enterprise Systems. These systems include: ACRS; SCIC CSS; HONet; HuRIS. Each system maintains their own individual PIA with all legal authorities documented, and listing the GSS's UUID within their individually maintained PIA.

Data from the enterprise (source) systems are stored on select network file shares and can include Social Security Number, Name, Date of Birth, E-Mail Address, Phone Numbers, Education Records, Mailing Address, Employment Status, Mother’s Maiden Name, Medical Records Number, Medical Notes, Photographic Identifiers.

Data, at rest and in transit between these systems and the GSS infrastructure is encrypted and follow strict Federal Information Processing Standards.

Users requiring access log in using NIH IAM which maintains its own 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.

Social Security Number
Date of Birth
Name
Photographic Identifiers
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Education Records
Employment Status

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

Employees
Public Citizens
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

Information is used for clinical research, clinical care, collaborating, scheduling and NIDA administrative functions.

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

There are no secondary uses for the data.

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

Public Health Service Act, 42 USC § 203, 241, 285o; 44 USC § 3101
5. U.S.C. 301; 42 U.S.C. 217a, 241, 282(b)(6), 284a, and 288. 48 CFR Subpart 15.3 and Subpart 42.15

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

No

09-25-0200; Clinical, Basic and Population-based Research Studies of the National Institutes of

09-25-0216 Administration: NIH Electronic Directory, HHS/NIH)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within the OPDIV

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

Section 301 of the Public Health Service Act, describing the general powers and duties of the Public Health Service relating to research and investigation (42 U.S.C. 241).

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 NIDA IRP GSS does not directly collect PII. Applications residing on the GSS can collect and store sensitive information or PII from NIH Enterprise systems. Each system maintains their own individual PIA with all legal authorities documented and lists the GSS's UUID within their individually maintained PIAs.

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.

All PII data is extracted from NIH Enterprise Systems.. Notification and consent from the individuals are provided at the time of collection from these systems.

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

All PII data is extracted from NIH Enterprise Systems.. Notification and consent from the individuals are provided at the time of collection from these systems.

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.

Users are instructed to contact NIDA Information Systems Security Officer (ISSO) or NIDA Privacy Coordinator for any security or privacy concerns.

Individuals can also contact the NIH Privacy Office 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.

Information in the system is derived from the NIH Enterprise systems,, NIDA relies on these systems to collect PII and maintain it.

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.

Access to the GSS and its applications is role based, and access is restricted to an individual users assigned role.

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 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).

Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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 Schedules.

10-101 - Administrative records maintained in any agency office.
Administrative records maintained in any agency office. Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists, excluding records scheduled elsewhere in the General Records Schedule (GRS) such as timekeeping and procurement. Disposition: Destroy when business use ceases. DAA-GRS-2016-0016-0001

001-003 - Records of All Other Intramural Research Projects.

These records do not meet the retention criteria for Item I-0001 - Records of Intramural Research Records or for Projects of Historical Significance, or Item I-0002 - Research Records that Support Intellectual Property Rights.

Intramural research records related to planning, development, oversight and execution of biomedical research projects and programs performed by NIH research staff, contractors or under collaborative research and development agreements (CRADAs).
Disposition: Cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer. Destroy 7 years after cutoff. DAA-0443-2012-0007-0003

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

Administrative Controls
System roles designate the level and nature of access a user can have and will employ the NIH single sign on capability. The system will provide an audit trail for user actions and log system access and system errors. The system has data checks to validate the accuracy of data in real time. All technical personnel who access information technology (IT) systems 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.

Physical Controls:
NIDA work areas are restricted to authorized employees and contractor personnel. The NIDA IRP GSS resides behind a firewall and is in a server room with no external access.
The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards. All personal not having card key access are escorted.

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.