US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/29/2024

OPDIV:

NIH

Name:

NIDA HQ General Support System

PIA Unique Identifier:

P-4867354-448062

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)?

Yes

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.

The National Institute on Drug Abuse (NIDA) Headquarters (HQ) General Support System (GSS) serves as a physical infrastructure that supports applications and services in support of the NIDA and NIH mission.

The system has now been determined to be an ad-hoc repository for Personally Identifiable Information (PII) within its network/data storage services allocated as individual or group network drive assignments.

Describe the purpose of the system.

The National Institute on Drug Abuse (NIDA) Headquarters (HQ) General Support System (GSS) provides a physical infrastructure that supports various applications and services in support of NIDA’ s mission. It also provides office automation and information processing services to NIDA research

and management programs.

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

The GSS is a physical infrastructure 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 and the like.

Applications/systems residing on the GSS can collect and store sensitive information or Personally Identifiable Information[ST1] (PII) Each system maintains their own individual Privacy Impact Assessment (PIA) and each subsystem will list the NIDA GSS' Universally Unique Identifier (UUID) within their respective PIA.

All PII data is extracted from the following NIH enterprise systems: Information for Management Planning, Analysis, and Coordination II (IMPAC II), NIH Enterprise Directory (NED), and NIH Business System (NBS).

The subsystems under the GSS include:
NIDA Extramural Project System (NEPS)
Drug Inventory Supply & Control System (DISCS)
Conference Approval System (CAS)
ATDP Information Management System (AIMS)
Livelink
NIDA Data Share
Clinical Data Repository

Data from the enterprise (source) systems can include Social Security Number, Name, Date of Birth, E-Mail Address, Phone Numbers, Education Records, Mailing Address, Employment Status and is stored on select network file shares.

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

Users requiring access log in using NIH Identity and Access Management Services (IAM) which maintains its own 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 enforce information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores 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 HQ GSS is a physical infrastructure consisting of security appliances, security tools, software life cycle management tools, networking devices, enterprise storage solutions, application hosting resources, enterprise communications services and therefore does not directly collect sensitive information or PII but can be used to store such information (e.g., financial, personnel, contractual, grant management) on select network file shares.

The following applications/systems residing within the NIDA HQ GSS can collect and store data extracted from NIH enterprise systems and include IMPAC II, NED, and NBS. These subsystems include:
NEPS
DISCS

CAS
AIMS
Livelink
NIDA Data Share
Clinical Data Repository

These systems maintain their own unique PIA, with all legal authorities documented. Each system under the GSS will list the GSS' UUID within their respective PIAs.

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

Users requiring access log in using NIH IAM Services, 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
E-Mail Address
Mailing Address
Phone Numbers
Education Records
Employment Status

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

Employees
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

Human Resources (HR)/Employment, Grant, and/or Acquisition Purposes.

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?

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.

09-25-0036 - Extramural Awards and Chartered Advisory Committees (IMPAC ll), Contract

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

09-25-0217 NIH Business System (NBS)

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

N/A 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 HQ GSS nor its hosted applications directly collect PII. All personal information data is extracted from NIH enterprise systems (IMPAC II, NED, and NBS which maintain their own unique PIA with all legal authorities documented.

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 (IMPAC II, NED, NBS). 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 (IMPAC II, NED, NBS). Consent from the individuals is 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.

Individuals can 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 will be derived from transfers from the NIH enterprise systems (IMPAC II, NED, NBS). 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.

Access to two of the hosted applications that contain business sensitive or PII is granted only to NIDA authorized personnel. The HQ GSS implements Multi Factor Authentication (MFA) and will provide the authentication and authorization of the user credentials. The system will enable a user to only perform actions specific to their role.

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 system is role-based and based on the role assigned to an individual user, the user may only access areas in the system restricted to the 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).

NIH identifies personnel with significant information system security roles and responsibilities, document those roles and responsibilities, and provide appropriate information system security training via the NIH training portal. Some role-based training courses that are provided are[TS([1] :
Systems Administrator Training
HHS Information Security for Executives
HHS Information Security for Managers
HHS Information Security for Information Technology (IT) 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 within the NIDA HQ GSS 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 GRS such as timekeeping and procurement. Disposition: Destroy when business use ceases. DAA-GRS-2016-0016-0001

02-004- Extramural Program and Grants Management Oversight Records
These records are generated during the administration and execution of extramural program activities. This schedule item is intended to capture all extramural program and grants management records that are not part of an official case file (Item 0001 or 0002) or animal welfare assurance file (Item 0003). These records support the operations, compliance, reporting, and oversight functions of the NIH Extramural Program and the financing of research endeavors with the purpose of ensuring

scientific integrity and public accountability of the NIH extramural research portfolio. Extramural program and grants management oversight records are consolidated under one common temporary retention item. Disposition: Cut off annually. Destroy 3 years after cutoff. DAA-0443-2013-0004-0004

06-208 - Employee performance file system record. Acceptable performance appraisals of non-senior executive service employees.
Employee performance file system record. Acceptable performance appraisals of non-senior executive service employees. Employee performance records are ratings of record, the performance plans on which ratings are based, supporting documentation for those ratings, and any other performance-related material required by an agency's performance appraisal system. Exclusion: Performance records of Presidential appointees are not covered by the GRS. Such records must be scheduled by submitting an agency-specific schedule to NARA. Disposition: Destroy no sooner than 4 years after date of appraisal, but longer retention is authorized if required for business use. DAA-GRS-2017-0007-0008

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

Physical Controls:
NIDA work areas are restricted to authorized employees and contractor personnel. The NIDA HQ 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.

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.

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.