US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/10/2025

OPDIV:

NIH

Name:

NHGRI IT GSS

PIA Unique Identifier:

P-1375655-249523

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

Significant System Management Change

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

This validation is intended to refresh content and update the status of the National Human Genome Research Institute (NHGRI) Information Technology (IT) Infrastructure general support system (GSS) Privacy Impact Assessment (PIA). Specifically, Labmatrix (classic and Chameleon) are being decommissioned. Data that resided in them are being moved to a Clinical Center managed REDCap (Research Electronic Data Capture) application. NHGRI-Druva was decommissioned March 19, 2025. It is not being replaced by another application.

Describe the purpose of the system.

The National Human Genome Research Institute (NHGRI) Information Technology (IT) Infrastructure general support system (GSS) is a Federal Information Security Modernization Act (FISMA)-Moderate and provides an infrastructure that supports applications and services in support of the

NHGRI's scientific mission. The NHGRI GSS provides automation and information processing services to NHGRI research and management programs. The NHGRI GSS supports approximately 800 users, including federal employees, direct contractors, visiting fellows, and special volunteers. The system is critical to NHGRI meeting its mission.

The NHGRI GSS supports the following minor applications.

Financial Strategic Planning System (FSPS)

Labmatrix (classic and Chameleon) – will be decommissioned and replaced by REDCap

NHGRI Acquia (cloud)

NHGRI Amazon Web Services (AWS) (cloud)

NHGRI TrakGene

NHGRI NIH Intramural Sequencing Center (NISC) Data Archive-Retrieval (NISCDAR) (cloud)

Undiagnosed Diseases Program Integrated Collaboration System (UDPICS)

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

The NHGRI GSS does not itself collect, maintain (store), or share information, aside from the following personally identifiable information (PII) for provisioning accounts and for communications, including automated notifications and alerts: name, email address, phone number, and/or organization. Users log into some NHGRI GSS tools/utilities with a tool/utility-specific user identifier (ID) and password.

The NHGRI GSS may also collect, maintain, and/or share the following types of non-PII:

Device identifiers (internet protocol (IP) address, asset tags, serial numbers)

File metadata (file name, size)

The NHGRI GSS supports minor applications that have unique and specific privacy impact assessments (PIAs) that address the types of information they will collect, maintain, store, and share, including PII. Each minor application will list the NHGRI GSS Universally Unique Identifier (UUID) within their respective PIAs.

The NHGRI GSS also hosts NHGRI internal and external Web sites that may collect, maintain (store), or share information. These Web sites have unique and specific PIAs (when required) that address the types of information they will collect, maintain, store, and share, including PII. Each Web site will list the NHGRI GSS UUID within their respective PIAs.

Users log into the NHGRI GSS using the NIH Identity, Credential, and Access Management (IAM) Services, which maintains its own unique PIA on record, including 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 stores them in an encrypted format. The IAM Services are an essential service that 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 NHGRI IT Infrastructure GSS is a FISMA-Moderate and provides a infrastructure that supports applications and services in support of the NHGRI's scientific mission. The NHGRI GSS provides automation and information processing services to NHGRI research and management programs. The NHGRI GSS supports approximately 800 users, including federal employees, direct contractors, visiting fellows, and special volunteers. The system is critical to NHGRI meeting its mission.

The NHGRI GSS supports the following minor applications.

Financial Strategic Planning System (FSPS)

Labmatrix (classic and Chameleon) – will be decommissioned and replaced by REDCap

NHGRI Acquia (cloud)

NHGRI Amazon Web Services (AWS) (cloud)

NHGRI TrakGene

NHGRI NIH Intramural Sequencing Center (NISC) Data Archive-Retrieval (NISCDAR) (cloud)

Undiagnosed Diseases Program Integrated Collaboration System (UDPICS)

The NHGRI GSS does not itself collect, maintain (store), or share information, aside from the following personally identifiable information (PII) for provisioning accounts and for communications, including automated notifications and alerts: name, email address, phone number, and/or organization. Users log into some NHGRI GSS tools/utilities with a tool/utility-specific user identifier (ID) and password.

The NHGRI GSS may also collect, maintain, and/or share the following types of non-PII:

Device identifiers (internet protocol (IP) address, asset tags, serial numbers)

File metadata (file name, size)

The NHGRI GSS supports minor applications that have unique and specific privacy impact assessments (PIAs) that address the types of information they will collect, maintain, store, and share, including PII. Each minor application will list the NHGRI GSS Universally Unique Identifier (UUID) within their respective PIAs.

The NHGRI GSS also hosts NHGRI internal and external Web sites that may collect, maintain (store), or share information. These Web sites have unique and specific PIAs (when required) that address the types of information they will collect, maintain, store, and share, including PII. Each Web site will list the NHGRI GSS UUID within their respective PIAs.

Users log into the NHGRI GSS using the NIH Identity, Credential, and Access Management (IAM) Services, which maintains its own unique PIA on record, including 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 stores them in an encrypted format. The IAM Services are an essential service that facilitates and governs network access to various resources.

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
Phone Numbers
Organization
Tool/utility-specific user credentials (ID and password)

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?

500-4,999

For what primary purpose is the PII used?

PII is only used for provisioning accounts and for communications, including automated notifications and alerts.

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.

42 USC 241; 42 USC 282; 42 USC 284; 42 USC 285s

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.

Published - 09-90-0777, Facility and Resource Access Control Records

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Government Sources
Within the OPDIV

Identify the OMB information collection approval number and expiration date

Not applicable. An Office of Management and Budget (OMB) collection approval number is not needed as the NHGRI GSS only uses the PII of federal employees (or direct contractors with NIH badges) for internal use only.

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 PII collected and used for provisioning accounts comes from the NIH Enterprise Directory (NED). NED maintains its own PIA outlining the process to notify individuals that their PII is collected.

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 option to opt-out. The collected information is from NED. NED collects the PII during the hiring process. An individual may decline to give their PII, but that would remove them from the hiring process.

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

The NHGRI GSS is not the source system for the PII of employees/contractors with provisioned accounts. The PII comes from NED. NED maintains a process to notify and obtain consent from individuals when a major change occurs. NED 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.

The NHGRI GSS is not the source system. NED is the source system and maintains processes for individuals to resolve concerns about their PII. NED maintains its own PIA.

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

The NHGRI GSS is not the source system. NED is the source system and maintains processes for periodic reviews of PII in NED. NED 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.

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.

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 PII is assigned to personnel based upon current job responsibilities. An NIH IAM Services account login is required to gain access. For some tools/utilities, a tool/utility-specific user ID and password is required to gain access.

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).

Administrators and Privileged users require additional training specific to their roles and responsibilities. As well as for individuals with significant security 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.

Login /Systems Access Records are retained and disposed of under the authority of the following NIH Records Schedule:Item 07-203: System Access Records. Systems not requiring special accountability for access.Destroy when business use ceases (Disposition Authority DAA-GRS-2013-0006-0003).

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

Administrative: The system had a security assessment and authorization (SA&A) performed in accordance with NIH and HHS requirements. SA&A documentation including the following were developed as required: security categorization, e-authentication risk assessment, system security plan, evidence of security control testing, and plan of action and milestones. Applicable Privacy Act clauses are inserted in solicitations and contracts as applicable. Policies for the retention and destruction of PII are in place. The NHGRI Information Technology Branch performs backups of system data on a regular basis.

Technical Controls: User authentication services are provided by the NIH IAM Services. Users log into some NHGRI GSS tools/utilities with a tool/utility-specific ID and password. Roles are used to control who has access to PII. Intrusion detection is provided by the NIH network at the perimeter and other points within the network. The NIH Incident Response Team is responsible for incident handling, response, and reporting, and will notify the NHGRI Information Systems Security Officer of any incidents that can be related to the system.

Physical Controls: System components are in NIH data centers, which have appropriate physical controls to restrict access to servers. Access to data centers is controlled by NIH Personal Identity Verification card. Visitors are always escorted."