US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/06/2025

OPDIV:

NIH

Name:

Genetic Testing Registry

PIA Unique Identifier:

P-1907729-625564

The subject of this PIA is which of the following?

Minor Application (child)

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?

Yes

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.

This validation is intended to refresh content and update the Point of Contact. There have been no substantial changes since the last assessment.

Describe the purpose of the system.

The NIH Genetic Testing Registry (GTR) is a public database that health care providers, researchers, and others can use to search for clinical, and research genetic tests and laboratory information submitted voluntarily by test providers. The GTR enhances access to information about the availability and scientific basis of genetic tests, including newer types of tests such as pharmacogenomic and liquid biopsy tests.

The GTR provides information about clinical and research tests for heritable variants, including biochemical and pharmacogenomic tests, tests for somatic variants, and tests for chromosomal aberrations and copy number variants, as well as information about the laboratory offering the test,

such as contact information and credentials of the laboratory (e.g., certification and licensure).

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

The Personally Identifiable Information (PII) collected, maintained or shared within the GTR includes the laboratory's point of contact's credentials, including Name, Email Address, Phone Number, and Mailing Address.

Also captured is test information (the purpose of the test and its limitations, whether it is a clinical or research test, the test methodology and analytes that are measured, performance characteristics such as analytic validity and clinical validity, information on clinical utility, and whether manufactured tests have been cleared or approved by the Food and Drug Administration).

NIH users log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with all legal authorities documented. Login for partnered labs and institutions is done through NIH IAM Services' Federated login. 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 NIH Genetic Testing Registry (GTR) is a public database that health care providers, researchers, and others can use to search for clinical, and research genetic tests and laboratory information submitted voluntarily by test providers. The GTR enhances access to information about the availability and scientific basis of genetic tests, including newer types of tests such as pharmacogenomic and liquid biopsy tests.

The GTR provides information about clinical and research tests for heritable variants, including biochemical and pharmacogenomic tests, tests for somatic variants, and tests for chromosomal aberrations and copy number variants, as well as information about the laboratory offering the test, such as contact information and credentials of the laboratory (e.g., certification and licensure).

The PII collected, maintained or shared within the GTR includes the laboratory's point of contact's credentials, including Name, Email Address, Phone Number, and Mailing Address.
Also captured is test information.

NIH users log in using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented. Login for partnered labs and institutions is done through NIH IAM Services' Federated login.

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
Mailing Address
Phone Numbers
Test information

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?

500-4,999

For what primary purpose is the PII used?

The primary purpose for the use of PII is to provide users information about laboratories offering tests, including points of contact.

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 U.S.C. section 286, 42 U.S.C. § 282(i) and (j)), 44 U.S.C. Sec. 2904, 42 U.S.C. 241.

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.

09-25-0200; Clinical, Basic and Population-based

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Government Sources
Within the DOC
Non-Governmental Sources
Public
Private Sector

Identify the OMB information collection approval number and expiration date

0925-0651, January 31, 2025 (in review for update)

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 list of fields available for collection is provided to both individuals submitting PII information and the general public. Individuals submitting PII information are shown the Office of Management and Budget (OMB) burden statement and approval information for review. Additionally, submitters are required to review and agree to a code of conduct statement before submitting PII information.

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.

Individuals have the option to not enter their PII during the registration process. However, failure to enter PII will result in not being able to enter a lab's information into the system.

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

Individual submitters are notified of changes to their personal and/or personally submitted PII data via automated emails or personal emails/calls from GTR staff. Major changes are relayed via automated emails or other notifications to database participants, personal emails/calls from GTR staff, or notification on the public website. When notifications are done via email, GTR staff follow-up personally (by phone or email) with any users in which the email bounced to ensure the message has been received. Notifications include information on what was changed and how to accept, reject, or edit any changes.

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 GTR employs a Standard Operating Procedure (SOP) for Resolution of Complaints about information submitted to the Genetic Testing Registry through the “Contact GTR” link on the GTR homepage. This link brings the user to a feedback form, which includes options to “report information that appears to be inaccurate or misleading” and to submit “other comments or questions on the content of the registry.”

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

Periodic data integrity audits are conducted by GTR Administrative Staff.

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.

Periodic review of system users' roles are done to assure access is current with user's technical/functional role in administering, developing, and supporting the daily job functions of the GTR.

An IAM account login is required to gain access to the stored PII data.

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).

The GTR maintains tutorials on YouTube for the public. Standard Operating Procedures exist for internal system users.

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 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-GRS2016-0016-0001

Item 07-204 -System access records; Systems requiring special accountability for access.
These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
Disposition: Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. DAA-GRS- 2013-0006-0004

Item 07-201 Systems and data security records;
These are records related to maintaining the security of information technology (IT) systems and data.
Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific
systems for which they were written. This series also includes analysis of security policies, processes, and
guidelines, as well as system risk management and vulnerability analyses.
Disposition: Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/information technology (IT) administrative purposes to ensure a continuity of security controls throughout the life of the system. DAA-GRS-2013-0006-0001

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

Administrative Controls: System users are approved by GTR's management for access based on their technical/functional role in administering, developing, and supporting GTRS' daily job functions, and GTR administrators perform periodic reviews to assure users adhere to system policies.

Technical Controls: Access to the system is controlled by NIH IAM Services which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. 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 integrity of data.

Physical Controls: The servers reside in the National Library of Medicine (NLM) Data Center where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.

Identify the publicly-available URL:

https://www.ncbi.nlm.nih.gov/gtr/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes