US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/26/2025

OPDIV:

NIH

Name:

NHGRI TrakGene

PIA Unique Identifier:

P-3390255-836227

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?

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 NHGRI TrakGene Clinical Genetics Information Management Solution (TrakGene) has been developed specifically to assist in the clinical and administrative management of genetic disorders, including cancer genetics. NHGRI TrakGene allows linking of families (pedigree) for effective and efficient management by the clinical team.
Functions include recording, analyzing, retrieving and reporting clinical information, from demographic data to diagnosis, to study participants and appointment management, managing diet plans and pedigree drawing.

The PIA was last approved external to the HHS system. Since then it has been updated to meet the requirements of Executive Order - Defending Women From Gender Ideology Extremism And Restoring Biological Truth To The Federal Government.

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

NHGRI TrakGene collects study participant data along with details of other family members.

Personally identifiable information (PII) stored includes name, mother's maiden name, e-mail address, phone numbers, medical notes, education records, date of birth (DOB), biometric identifiers, mailing address, medical records number (MRN), sex, demographic information, highest level of education, and income (financial account information). Referrals, appointments, investigations, diagnoses, and notes are also stored.

Social security numbers (SSN) could be included in the notes field for use in conjunction with the Clinical Center's (CC) travel system for arranging travel, lodging, and vouchers for study participants. The CC Travel system maintains its own unique privacy impact assessment (PIA), with all legal authorities documented.

Users log in with an NHGRI TrakGene user identifier (ID) and password.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The NHGRI TrakGene Clinical Genetics Information Management Solution (TrakGene) has been developed specifically to assist in the clinical and administrative management of genetic disorders, including cancer genetics. NHGRI TrakGene allows linking of families (pedigree) for effective and efficient management by the clinical team.
Functions include recording, analyzing, retrieving and reporting clinical information, from demographic data to diagnosis, to study participants and appointment management, managing diet plans and pedigree drawing.

NHGRI TrakGene collects study participant data along with details of other family members. Personally identifiable information (PII) stored includes name, mother's maiden name, e-mail address, phone numbers, medical notes, education records, date of birth (DOB), biometric identifiers, mailing address, medical records number (MRN), sex, demographic information, highest level of education, and income (financial account information). Referrals, appointments, investigations, diagnoses, and notes are also stored.

Social security numbers (SSN) could be included in the notes field for use in conjunction with the Clinical Center's (CC) travel system for arranging travel, lodging, and vouchers for study participants. The CC Travel system maintains its own unique privacy impact assessment (PIA), with all legal authorities documented.

Users log in with an NHGRI TrakGene user identifier (ID) and password.

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
Biometric Identifiers
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Education Records
demographic information, sex, highest level of education

Referrals, appointments, investigations, diagnoses, and notes
NHGRI TrakGene User Credentials (ID and password)

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

NHGRI TrakGene is used to record, document, and analyze clinical information.
NHGRI TrakGene user credentials are used to control access to the system.

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.

45 CFR 46; 42 USC 241; 42 USC 281; 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.

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Person
Email
Government Sources
Within OpDiv
Non-Government Sources
Public

Identify the OMB information collection approval number and expiration date

Not Applicable. Public Law 114-255, Section 2035, exempts research conducted by NIH from PRA paperwork reduction Act requirements.

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.

Study participants provide/document their consent with an NIH Institutional Review Board (IRB)-approved consent form. The consent form states that medical information will be stored in NIH medical information systems.

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.

Participation in clinical studies is voluntary; however, PII/PHI is required for clinical research/participation. Should a participant opt-out of providing the required PII, the participant is in effecting opting out of the entire study.

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

When an initiative arises in which historical data or specimens are desired for use in ways not covered by prior consent, the IRB reviews and advises on the scope of consent. In many cases, the NIH IRB requires re-consent with the study participant or requires that program refrain from data or specimen uses not previously consented.

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 process to resolve individual's concerns about their PII and how it is being used is done through the Principal Investigator (PI) leading each case study and the NIH IRB. Participants may reach out to their respective PI via email or phone; and work with them to correct any issues.

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 reviews of PII contained within the system are performed by the PI overseeing the clinical study and the NIH IRB.

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 NHGRI TrakGene 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.

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

Describe training system users receive (above and beyond general security and privacy awareness training).

Additional training is required 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.

Study participant records pertaining to NHGRI TrakGene are retained and disposed of under the authority of the following NIH Records Schedule: 01-003: Records of All Other Intramural Research Projects.

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

Disposition Instructions: 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

Login/System Access Records are retained and disposed of under the authority of the following NIH Records Schedule: 07-203: System access records. Systems not requiring special accountability for access.

System Access Records. 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.

Exclusion 1: Excludes records relating to electronic signatures.

Exclusion 2: Does not include monitoring for agency mission activities such as law enforcement.

Systems not requiring special accountability for access. These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users.

Disposition Instructions: Destroy when business use ceases. 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: NHGRI TrakGene is undergoing a security assessment and authorization (SA&A) performed in accordance with NIH and HHS requirements. SA&A documentation including the following are being 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. NHGRI IT Branch (ITB) performs backups of system data on a regular basis.

Technical: Users authenticate to NHGRI TrakGene with a NHGRI TrakGene user ID and password. Access to PII is assigned to personnel based upon current job responsibilities. Logical access controls restrict access to the servers hosting the system to only those administrators requiring access to maintain the servers and the NHGRI TrakGene application.

Intrusion detection is provided by the NIH network at the perimeter and other points within the network. The NIH Information Response Team is responsible for incident handling, response, and reporting, and will notify the NHGRI Information System Security Officer of any incidents that may be related to the system.

Physical: System components are located in NIH data centers, which have appropriate physical control to restrict access to servers. Access to data centers is controlled by NIH