US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/29/2024

OPDIV:

NIH

Name:

(NIAID) Clinical Genomics Systems

PIA Unique Identifier:

P-3103280-697159

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 systems within the National Institute of Allergies and Infectious Diseases (NIAID) Clinical Genomics Systems Boundary are collaboration based systems designed to aid in the study of genomics data in order to further the knowledge base of personalized medicinal approaches in human health and disease.

Genomic Research Integration System (GRIS) is a web-based, application that was developed to identify causal genetic variants of immunological disorders. GRIS provides systematic and automated capturing and linking of patient clinical and genomic data from disconnected systems accompanied by standardized annotations to enable cross comparisons across data from different clinical studies. Data access, analysis, and sharing workflows have been optimized to promote maximum data usage while protecting patient privacy and confidentiality.

Seqr@NIAID is used for analysis of genomic data sets by and for individual NIAID Investigators. These data sets are de-identified and are not meant for sharing amongst investigators. Seqr@NIAID

allows investigators to perform exploratory screening of data sets before determining whether to pursue them further and boutique analysis of data sets. Data is obtained by an investigator through collaborations.

Host Genetics Repository (HGRepo) is a web-based portal used by NIAID Division of Intramural Research Principal Investigators (PI) and their research teams to enable collaborative access to comprehensive and standardized clinical and sample biomedical data. HGRepo provides a structured repository for study data including patient information (including personally identifiable information (PII), as well as phenotypic, hospitalization, treatment, clinical laboratory and omics assay, and sample data. Users can add their own datasets and sample registries and extend and curate them in HGRepo. In this way users can use HGRepo to join their own data to data received from other systems such as the Clinical Research Information Management System of NIAID (CRIMSON), which . HGRepo provides users with graphical tools to explore, connect, and export their data as well as downloadable scripts for savvy users to access the data via the LabKey Application Programming Interface (API) from their own workstations or environment(s).

Structural Annotation and Visualization (SUNLIT) enables researchers to visualize the location of a genetic variant on a 3-D protein structure that highlights the residue(s) impacted by the variant and thus facilitates analysis of candidate variants and identification of disease variants. No sensitive information is contained within this application nor included in any traffic to/from this application. The SUNLIT application is deployed within the Monarch infrastructure.

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

GRIS and HG Repo contain PII from the public. Patient encounter information including medical histories (notes), examinations, treatment plans, interventions, and the outcomes of those interventions. Other PII collected include medical records number (MRN), date of birth. Documentation of family histories and health events may include identifiers of both the individual and family members, such as mother's maiden name. Common contact information including name, mailing address, phone number, e-mail address.

NIAID personnel who log in to this system 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. 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 which facilitates and governs network access to various resources.

User work related contact information is retained within the applications (name, work email address) for access control purposes and research association.

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

The systems within the National Institute of Allergies and Infectious Diseases (NIAID) Clinical Genomics Systems Boundary are collaboration based systems designed to aid in the study of genomics data in order to further the knowledge base of personalized medicinal approaches in human health and disease.

Genomic Research Integration System (GRIS) is a web-based, application that was developed to identify causal genetic variants of immunological disorders. GRIS provides systematic and automated capturing and linking of patient clinical and genomic data from disconnected systems accompanied by standardized annotations to enable cross comparisons across data from different clinical studies. Data access, analysis, and sharing workflows have been optimized to promote maximum data usage while protecting patient privacy and confidentiality.

Seqr@NIAID is used for analysis of genomic data sets by and for individual NIAID Investigators. These data sets are de-identified and are not meant for sharing amongst investigators. Seqr@NIAID allows investigators to perform exploratory screening of data sets before determining whether to pursue them further and boutique analysis of data sets. Data is obtained by an investigator through collaborations.

Host Genetics Repository (HGRepo) is a web-based portal used by NIAID Division of Intramural Research Principal Investigators (PI) and their research teams to enable collaborative access to comprehensive and standardized clinical and sample biomedical data. HGRepo provides a structured repository for study data including patient information (including personally identifiable information (PII), as well as phenotypic, hospitalization, treatment, clinical laboratory and omics assay, and sample data. Users can add their own datasets and sample registries and extend and curate them in HGRepo. In this way users can use HGRepo to join their own data to data received from other systems such as the Clinical Research Information Management System of NIAID (CRIMSON). HGRepo provides users with graphical tools to explore, connect, and export their data as well as downloadable scripts for savvy users to access the data via the LabKey Application Programming Interface (API) from their own workstations or environment(s).

Structural Annotation and Visualization (SUNLIT) enables researchers to visualize the location of a genetic variant on a 3-D protein structure that highlights the residue(s) impacted by the variant and thus facilitates analysis of candidate variants and identification of disease variants. No sensitive information is contained within this application nor included in any traffic to/from this application. The SUNLIT application is deployed within the Monarch infrastructure.

GRIS and HG Repo contain PII from the public. Patient encounter information including medical histories (notes), examinations, treatment plans, interventions, and the outcomes of those interventions. Other PII collected include medical records number (MRN), date of birth. Documentation of family histories and health events may include identifiers of both the individual and family members, such as mother's maiden name. Common contact information including name, mailing address, phone number, e-mail address.

NIAID personnel who log in to this system 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. 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 which facilitates and governs network access to various resources.

User work related contact information is retained within the applicat

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Date of Birth
Name
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes

Medical history - examinations, treatment plans, interventions, outcomes of the interventions
Family medical history
Username
Password

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

Employees
Public Citizens
Patients

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

PII is used to identify the patient and linking them to research findings.

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

PII may be used during system development and testing activities. Access control purposes for NIAID users.

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 285f

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.

09-25-0099, Clinical Research: Patient Medical Records, HHS/NIH/CC

Identify the sources of PII in the system.

Government Sources
Within OpDiv
Non-Governmental Sources
Public

Identify the OMB information collection approval number and expiration date

NIH research activities are exempt from an OMB Information Collection Number through Public Law 114-255 - 21st Century Cures Act, Section 2035: Exemption for the National Institutes of Health from the 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.

PII is sourced from CRIMSON and Clinical Research Information System (CRIS) systems, which maintain their own PIAs, and is uploaded by the research teams from local files (provided to researchers by their collaborators). Individuals whose PII is imported to Clinical Genomics Systems provide consent for research purposes to the participating NIH Institute or Center. Individuals sign an informed consent protocol form that advises of their information being used for research purposes.

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.

The individual must contact the applicable NIH Institute or Center that collected the individual's original consent to request that their data be removed. PII is retained as part of research data unless specifically requested to be removed by the protocol owner, primary investigator, or the owner of the PII.

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

CRIMSON and CRIS, which maintain their own PIAs, are the data sources. Clinical Genomics Systems import data from CRIMSON and CRIS daily. Individuals use the process established CRIMSON and CRIS to obtain consent from individuals when major change occurs.

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 individual must contact the applicable NIH Institute or Center that collected the individual's original consent to address any issues regarding PII. If corrections are required, once CRIMSON or CRIS, which maintain their own PIAs, are updated, the data in Clinical Genomics Systems shall reflect the update on the next daily refresh.

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

PII is imported into Clinical Genomics Systems from the CRIMSON and CRIS systems daily and uploaded by the research teams from local files (provided to researchers by their collaborators). CRIMSON, CRIS, and collaborators are responsible for the collection of PII and are responsible for implementing a process for periodic reviews of PII contained in their systems to ensure the data's integrity, availability, accuracy, and relevancy prior to being shared with Clinical Genomics Systems.

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.

Roles/groups are designated by least privilege and therefore restrict the actions that can be taken and information that can be viewed by a user based on role/group membership. Assignment to any role or group is subject to approval by project leads.

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.

Roles/groups are designated by least privilege and therefore restrict the actions that can be taken and information that can be viewed by a user based on role/group membership.

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.

The National Institutes of Health (NIH) Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel who manage or operate NIH applications must successfully complete training at the onset of their employment and annually thereafter. Information Security and Privacy Awareness 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 provided role-based training for developers and administrators.

GRIS users must complete Office of Human Subjects Research Protection Training prior to being granted access. GRIS also offers informal introductory or advanced training related to usage of the system.

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.

Patient records are retained and disposed of under the authority of the NIH Intramural Records Schedule, Item I-0003: Records of All Other Intramural Research Projects. These are temporary records, cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer. Destroy 7 years after cutoff.
[Disposition Authority: DAA-0443-2012-0007-0003]

Login /Systems Access Records are retained and disposed of under the authority of the General Records Schedule, Section 3.2.030: System Access Records. These are temporary records. 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.

Physical: Systems in the Clinical Genomics Boundary hosted at the NIAID Office of Cyber Infrastructure and Computational Biology (OCICB) facility located at 5601 Fishers Lane, Rockville MD, 20852. Physical access to the property is managed by the OCICB Computing Facility Operations Team and requires an NIH Badge, which must be obtained through a vetting process, or an arranged escort into building.

Technical: Access to the hosting environment is managed by the Operations and Engineering Branch (OEB). Only designated staff of the OCICB OEB are granted access to hosting systems. Designated users of systems withing the Clinical Genomics Systems boundary must gain access through the use of multi-factor authentication by using issued NIH PIV cards, usernames and passwords, authenticator applications, and encryption of data in transit and at rest. Access to PII is monitored.

Administrative: National Institutes of Health (NIH) staff, including direct contractors take mandatory security and privacy training. Access is via least privilege through role-based access, and policies for retention of PII are in place. 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. Contract clauses ensure adherence to privacy provisions and practices.