US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/11/2025

OPDIV:

NIH

Name:

NEI OpenSpecimen

PIA Unique Identifier:

P-1413923-035607

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?

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. There have been no substantial changes since the last assessment.

Describe the purpose of the system.

The National Eye Institute (NEI) OpenSpecimen is a biobanking informatics software that offers a complete solution for all aspects of the biobanking workflow from donor consent, biospecimens collection, to request and distribution. It allows annotation of clinical data associated with the biospecimens and tracking of the complete lifecycle of a biospecimen.

A biobank is a type of biorepository that stores biological samples (usually human) for use in research. Biobanks have become an important resource in medical research, supporting many types of contemporary research like genomics and personalized medicine.

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

Information collected in OpenSpecimen will comprise of data relevant to the identification of patient samples, their collection, storage, analysis and results. This includes patient name, mother's maiden name, date of birth, medical records number and basic genetic information. It will also include information on diagnosis and other relevant disease data. NIH clinicians and scientists will use this information for clinical research.

Those requiring access to this system 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. 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.

OpenSpecimen is a biobanking informatics software that offers a complete solution for all aspects of the biobanking workflow from donor consent, biospecimens collection, to request and distribution. It allows annotation of clinical data associated with the biospecimens and tracking of the complete lifecycle of a biospecimen. OpenSpecimen allows annotation of clinical data associated with the biospecimens and tracking of the complete lifecycle of a biospecimen.

Information collected includes patient name, mother's maiden name, date of birth, medical records number and basic genetic information. It will also include information on diagnosis and other relevant disease data. NIH clinicians and scientists will use this information for clinical research.

Users log in to this system using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), which maintains its own unique privacy impact assessment (PIA) on record, including 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.

Date of Birth
Name
Mother's Maiden Name
Medical Records Number
Medical Notes
Basic genetic information
Diagnosis and other relevant disease data

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

Public Citizens
Patients

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

Sample data remains linked to clinical records so that the database can be used for secondary research studies.

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

No secondary use is planned, but there may be future research purposes, which would be submitted for review and approval through the institutional review board as required.

Identify legal authorities governing information use and disclosure specific to the system and program.

42 U.S.C. 241, 248, 281, 285i, and 44 U.S.C. 3101

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.

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Non-Government Sources

Public

Other

Identify the OMB information collection approval number and expiration date

Pub L Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) 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.

Patients are made aware that personally identifiable information (PII) will be collected during their visit to the clinic and sign an information practices form.

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.

A written, signed consent form is required for patients to participate in the studies from which their samples originate. The consent form must be signed to participate. There is an option to object to the information collection that will result in exclusion from the study.

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

Patients are processed within the NIH Clinical Center (CC). The notification process is handled according to CC rules and is situational based on the type of change to the system.

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 may contact the appropriate official (e.g., System Manager) and reasonably identify the record, specify the information to be contested, and state the corrective action sought and reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant. The right to contest records is limited to information which is incomplete, irrelevant, incorrect, or untimely obsolete.

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

No formal, periodic reviews are conducted to ensure data integrity. Once information is entered into the patient's medical record, it remains there and it is assumed that all information was relevant at some point. Patients confirm contact information at each visit to ensure accuracy of that information. Occasionally, the NEI Clinic will contact participants using the PII contained in the database to inform the participants of and/or gather additional consent for additional research studies for which they may be eligible or secondary research studies in which their samples may be included. At that time, accuracy of the PII is reviewed.

Several backup strategies are in place to ensure data availability. Snapshots of the virtual machine/s are taken for quick recoveries and to roll back to specific points in time. Nightly backups are performed on the virtual machine/s utilizing the Veeam backup solution. The backups are stored in a separate location from the production environment.

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 is limited to those with a legitimate business/mission need (need-to-know). Technical support personnel have access as necessary to perform their duties. When direct contractors access the system they are supervised. The system provides an automatic warning message when data is prepared for download.

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.

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 personally identifiable information necessary to perform their job.

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.

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).

Personnel receive training noted above. Personnel with special roles (e.g., technical, managers, executives) receive role-based training.

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 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 or for Projects of Historical Significance, or Item I-0002 - Research Records that Support Intellectual Property Rights.

Intramural research records related to planning, development, oversight and execution of biomedical research projects and programs performed by NIH research staff, contractors or under collaborative research and development agreements (CRADAs).
Disposition: 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)

Item 03-001 – Clinical Care Services Records
These records consist of clinical care services and clinical care department operational records that are consolidated under this one common temporary retention item. Exclusions and exceptions are noted and cross referenced to their appropriate item numbers within this schedule.
Disposition: Cut off annually at end of fiscal year. Destroy 7 years after cutoff. (DAA-0443-2019-0001-0001)

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

Administrative safeguards: NIH staff, including direct contractors take mandatory security and privacy training and include system security and contingency plan. Access is via least privilege through role-based access, and policies for retention and destruction 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. Files are backed up regularly and stored offsite. Contract clauses ensure adherence to privacy provisions and practices.

Physical Safeguards: Physical access to the system is controlled by security guards, employee badging, proximity cards, card readers, and security cameras. Access to the server is controlled by card readers at the server room door. There is a battery backup for power until the backup generator starts. Fire protection including sprinklers, and flooding sensors at the floor level.

Technical Controls: Technical Safeguards include restricting files using secure socket layer encryption, a two-factor authentication and role-based access controls.