US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/07/2025

OPDIV:

NIH

Name:

NEI Outpatient Eye Clinic (OEC)

PIA Unique Identifier:

P-4766832-435865

The subject of this PIA is which of the following?

Major Application

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

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

The PIA 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 purpose of the system.

The National Eye Institute (NEI) maintains a state-of-the art Outpatient Clinic within the NIH Clinical Center (CC) for the conduct of clinical trials in eye disease. The NEI Outpatient Clinic uses myriad electronic testing devices and imaging devices for medical diagnostics and research data collection, and an electronic medical record for clinical/research documentation. The Outpatient Eye Clinic (OEC) system integrates the data collected within the NEI Outpatient clinic from disparate vendor systems and interfaces with the NIH CC systems for intake of demographic data and export of visit summaries. This system provides paperless access to the ophthalmic clinical and research record to all NEI clinical personnel and authorized clinical trial staff. The implementation of modern data management and imaging warehouses and the integration of the medical devices with these

storehouses of information is important to the conduct of the modern clinical trial as well as care of the patients at NEI.

All components of the system are maintained on NEI managed equipment located on the NIH campus and accessible only from the NIH network.
The major components are:

The NextGen Electronic Health Record (EHR) is a commercial product from NextGen Healthcare, Inc. which has been customized to collect ophthalmic clinical and research data within the NEI Outpatient Clinic.

The Zeiss FORUM system is an ophthalmic imaging picture archiving and communication system (PACS) which collects imaging data from the clinic's Zeiss devices (Visual Fields, optical coherence tomography (OCTs), IOLMaster (intraocular lens)) as well as other interfaced devices. The FORUM PACS serves as the central storage location for images from the Zeiss, Heidelberg, Ophthalmic Labs, moniteur de champ visual (MonCV) and Optos systems.

The Ophthalmic Labs system is a database of images which are collected from Ophthalmic Labs cameras. These images are also exported to FORUM.

The Heidelberg system is a database of images collected from the Heidelberg ophthalmic imaging cameras. This system also transmits data to the FORUM PACS.

The Optos system is a database of images from the Optos cameras, exported, when possible, to the FORUM PACS system.

The Metrovision system is a database of data and images from the MonCV perimeters (a projection perimeter used for eye exams), which also exports to FORUM.

The Merge EyeCare PACS is a collection of historical images used for research and reference for clinical care.

The Progeny system is genetic pedigree software used to collect pedigree information from trial participants to better understand genetic transmission of disease.

Copies of reports from the Metrovision and Progeny systems are uploaded into the NextGen EHR. Interfaces between the EHR and the other major components decrease patient identification errors and allow clinical personnel a comprehensive view of the patient's clinical presentation at the visit.

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

The NEI OEC system stores ophthalmic clinical data and research data. This includes:
Name, email address, phone number(s), medical notes, foreign activities, Date of Birth (DOB), photographic and biometric identifiers, mailing address Medical records number (MRN), and medical history.

Raw data and messages are imported from the Clinical Center electronic medical record (EMR), raw and summary data from the medical instruments as well as clinical evaluation and patient demographic information is stored. Portable Document Format (PDF) summaries of raw data that were collected are transmitted to the NIH Clinical Center system.

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 the IAM 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 collects unique usernames and passwords (user credentials) and stores them in an encrypted format. The IAM 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.

NEI maintains a state-of-the art Outpatient Clinic within the NIH CC for the conduct of clinical trials in eye disease. The NEI Outpatient Clinic uses myriad electronic testing devices and imaging devices for medical diagnostics and research data collection, and an electronic medical record for clinical/research documentation. The OEC system integrates the data collected within the NEI Outpatient clinic from disparate vendor systems and interfaces with the NIH CC systems for intake of demographic data and export of visit summaries. This system provides paperless access to the ophthalmic clinical and research record to all NEI clinical personnel and authorized clinical trial staff. The implementation of modern data management and imaging warehouses and the integration of the medical devices with these storehouses of information is important to the conduct of the modern clinical trial as well as care of the patients at NEI.

All components of the system are maintained on NEI managed equipment located on the NIH campus and accessible only from the NIH network.
The major components are the NextGen Electronic Health Record (EHR), the Zeiss FORUM system, the Ophthalmic Labs system, the Heidelberg system, the Optos system, the Metrovision system, the Merge EyeCare PACS, and the Progeny system.

Copies of reports from the Metrovision and Progeny systems are uploaded into the NextGen EHR. Interfaces between the EHR and the other major components decrease patient identification errors and allow clinical personnel a comprehensive view of the patient's clinical presentation at the visit.

The NEI OEC system stores ophthalmic clinical data and research data. This includes:
Name, email address, phone number(s), medical notes, foreign activities, DOB, photographic and biometric identifiers, mailing address, MRN, and medical history.

Raw data and messages are imported from the CC EMR, raw and summary data from the medical instruments as well as clinical evaluation and patient demographic information is stored. PDF summaries of raw data that were collected are transmitted to the NIH Clinical Center system.

Those requiring access to this system log in using the NIH IAM Services which maintains its own unique PIA on record, with 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
Photographic Identifiers
Biometric Identifiers
E-Mail Address

Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Foreign Activities
Medical History
Patient demographics, PDF summaries of raw data

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?

100,000-999,999

For what primary purpose is the PII used?

Clinical research and care

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

N/A

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

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107

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
- Hardcopy
- Email
- Other

Government Sources
- Within OpDiv
- State/Local/Tribal
- Foreign
- Other Federal Entities
- Other

Non-Governmental Sources
- Public
- Private Sector
- Other

Identify the OMB information collection approval number and expiration date

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

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

The NEI OEC has a memorandum of understanding (MOU) with the NIH Clinical Center. Medical Release of Information Forms are used to release information to patients and their physicians or designated recipients.

NEI OEC maintains a Memorandum of Understanding (MOU) with the NIH Clinical Center (CC) CRIS system effective through 08/31/2021.

Vendors are given access only incidentally when necessary to trouble-shoot systems or instruments, and only under observation. Support contracts include confidentiality agreements for this purpose.

Describe the procedures for accounting for disclosures.

The process of documenting disclosures is manual. The vast majority of disclosures are made through the NIH Clinical Center Medical Legal Department. All disclosures made directly from the NEI OEC are documented in separate tables (Microsoft Access, Excel, or paper) and are easily retrievable as necessary.

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 personal information 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.

Enrollment in clinical research is voluntary and the collection of PII and medical notes is necessary to conduct research and provide clinical care. Therefore, a patient may not opt out of the collection or use of their PII while participating in research at the NIH. Patients sign a consent form agreeing to provide the necessary information.

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

The notification process is managed by the NIH Clinical Center and is situational based on the type of change to the system. All patients are notified of information practices upon admission. Each patient would be advised at the time of the next admission about major system changes and the CC Information Practices Notice would be revised and provided to each patient again.

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.

An individual may contact the appropriate official at the address specified under Notification Procedure, and reasonably identify the record, specify the information being contested, and state corrective action sought, with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

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

Patients confirm contact information at each visit to ensure accuracy of their personally identifiable information. Once information is entered into a patient's medical record, it remains there. Backup strategies are in place to ensure data availability.

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 vendors access the system, they connect remotely to an individual system through a Federal Information Processing Standards (FIPS) compliant application and supervised by site personnel at all times. Vendors do not maintain their own log in, they connect to an active session of a logged in site employee using an approved remote access tool.). A vendor connecting on site is using either a temporary account or is working with site personnel present at the individual instrument. Connections are documented.

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 PII necessary to perform their job.

Initial access is restricted to the NEI Out-patient Building 10 (OP10) Clinic group. Access to file permissions, the terminal server, etc. are further restricted.

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).

All NEI personnel complete mandatory role-based training based upon responsibilities and access permissions. All system users sign a standard confidentiality agreement.

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: Research records are maintained within the NEI OEC for one year at termination of project/program or when no longer needed for scientific reference, whichever is longer. Records are destroyed 7 years after cutoff, unless requested continuation by the Institute system in accordance with the National Archives and Records Administration (NARA) approved disposition schedule: DAA-0443-2012-0007-0003

Item 01-004: FDA Regulated Research Records
These are records required by 21 CFR that pertain to the receipt, shipment, and other disposition of new or
investigational drugs or devices. FDA regulated research records include, but are not limited to, Investigational
New Drug (IND) applications, Investigational Device Exemptions (IDE) and New Drug Applications (NDA),
amendments, safety reports, annual reports, and drug dispositions.
Disposition: Records are maintained within the NEI OEC for one year after application is approved/disapproved, or if no new application is filed, after the study is completed/discontinued and FDA is notified of discontinuation or when no longer needed for business and scientific use, whichever is longer. Records are destroyed 3 years after cutoff, unless requested continuation by the Institute system in accordance with the National Archives and Records Administration (NARA) approved disposition schedule: DAA-0443-2012-0007-0004

Item 03-002: Radiology and imaging Records
These records are comprised of X-rays and other roentgenographic images produced by devices and procedures, such as body/head scans created by computerized transaxial tomography (CT).
Disposition: Imaging records are maintained within the NEI OEC in five year intervals after inactivity or when no longer needed for scientific reference, whichever is longer. Records are destroyed 60 years after cutoff, unless requested continuation by the Institute system in accordance with the National Archives and Records Administration (NARA) approved disposition schedule: DAA-0443-2012-0007-0007

Item 03-005: Patient Medical Records.
These records document admissions and medical treatment for a patient accepted in a research project. These records are the primary source of evaluation and analysis for either clinical care or clinical research study.
Disposition: Patient records are maintained within the NEI OEC for five years after inactivity. Records are destroyed when no longer needed for scientific reference in accordance with the National Archives and Records Administration (NARA) approved disposition schedule: DAA-0443-2012-0007-0010

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

Physical Controls: The information technology (IT) hardware used to host protected information is located in a secured datacenter facility. The facility is only open to authorized personnel whose

access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.