US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/10/2026

OPDIV:

NIH

Name:

CC Healthy Volunteer Online Registration

PIA Unique Identifier:

P-6885680-942143

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?

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 purpose of the healthy volunteer registry is to match potential research volunteers with current or upcoming clinical research studies at the NIH Clinical Center (CC). Joining the healthy volunteer registry is free and users can cancel their registration at any time.

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

The following personally identifiable information is collected from potential volunteers: Name, address, email, date of birth (DOB), phone, demographics (sex, ethnicity, race, height, weight, habits such as smoker), allergies, medical conditions, medications and any implants.

Users 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, including 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.

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

The purpose of the healthy volunteer registry is to match potential research volunteers with current or upcoming clinical research studies at the NIH CC. Joining the healthy volunteer registry is free and users can cancel their registration at any time.

The following personally identifiable information is collected from potential volunteers: Name, address, email, DOB, phone, demographics, allergies, medical conditions, medications and any implants.

Users log in to this system using the NIH IAM Services which maintains its own unique 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
E-Mail Address
Mailing Address
Phone Numbers
Demographics (sex, ethnicity, race, height, weight, habits such as smoker), allergies, implants, medications, medical conditions.

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

Employees
Public Citizens

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

For recruiting volunteers for clinical studies.

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

None

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

The legal authority to operate and maintain this Privacy Act records system is 42 U.S.C. §§ 241, 248, 282 and 284

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

Online

Non-Governmental Sources

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.

There are no agreements in place

Describe the procedures for accounting for disclosures.

Audit logs track where the information is shared.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Every volunteer is presented with a disclosure and privacy policy. They must agree to continue in order to provide 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.

Members of the public voluntarily enter their own information. If they do not wish to participate in registration for research, they may simply choose not to volunteer and remove their information.

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

All volunteers are notified of information practices upon acceptance. Each 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.

A Privacy Rights Complaint Form is available to individuals when they believe that their PII has been inappropriately used or disclosed. The CC Department of Clinical Research Informatics (DCRI) Privacy Office will review the complaint and coordinate with the NIH Office of the Senior Official for Privacy(OSOP) to respond to the concern. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC DCRI Privacy Office.

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

Accuracy: Volunteers are responsible for entering accurate/their correct information.

Integrity: The system ensures data stays same and not manipulated.

Availability: Data is accessible to authorized users when needed.

Relevancy: Not in place due to the volume of people entering data, making this a logistical impossibility.

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.

Appropriate access is granted to the system based on predefined roles and job descriptions, and administrative access is limited to authorized employees based on current roles. Dual factor authentication with NIH Personal Identity Verification (PIV) card and NIH IAM Services will occur at time of login to the NIH Network. System owners are responsible for creating the proper security groups within their systems with the applicable permissions for group members to enforce least privilege.

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).

New users are trained by an experienced peer.

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 03-008 - Clinical Care Administrative Support Records
These administrative records are associated with support activities related to executing work functions unique to a clinical care environment. These files are non-clinical in nature and do not include information that is maintained in patient medical records.
Disposition: Destroy when 3 years old, but longer retention is authorized if needed for business use.
DAA-0443-2018-0002-0001

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 public networks to prevent unauthorized or malicious access. Access to the system is controlled by NIH login which authenticates the user prior to granting 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.

Identify the publicly-available URL:

https://www2.cc.nih.gov/hvsignup/

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?

No

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

null