

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/06/2025

OPDIV:

NIH

Name:

CC: Research Volunteer System

PIA Unique Identifier:

P-9835501-502753

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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.

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 Clinical Center (CC) Research Volunteer Systems (RVS) is the primary research volunteer recruitment system for NIH Institute/Center (I/C) clinical research programs. RVS maintains information about individuals seeking to participate in NIH clinical research studies. The CC Office of Patient Recruitment (OPR) staff perform queries in RVS to identify potential research participants for NIH researchers. The system processes request for compensation to research volunteers.

CC RVS consists of two modules:

The RVS Contact Module is used by CC OPR call center staff to collect information over the phone from research volunteers. Health questionnaire responses are entered in RVS and queried to identify

potential volunteers for participation as research subjects in approved research protocols conducted at NIH. Information from the questionnaire is shared with the NIH research team who may contact volunteers to enroll them into studies.

The RVS Payment Module is used to process requests for compensation to volunteers by NIH research teams and authorization of payments to research volunteers.

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

The RVS stores information that includes volunteer name, date of birth, mailing address, email address, phone numbers, medical record numbers medical information/notes (allergies, current medications, self-reported medical history, sex, right/left hand dominance), and demographic information including, age, race, sex, and NIH clinical research protocol numbers. If selected for study participation that includes compensation, the NIH IC research team will collect their Social Security Number (SSN) and enter it into the RVS Payment Module to process payment for their services. RVS also stores the names of NIH staff approving compensation for research volunteers.

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.

RVS is the primary research volunteer recruitment system for NIH I/C clinical research programs. RVS maintains information about individuals seeking to participate in NIH clinical research studies. The CC OPR staff perform queries in RVS to identify potential research participants for NIH researchers. The system processes request for compensation to research volunteers.

RVS consists of two modules:

The RVS Contact Module is used by CC OPR call center staff to collect information over the phone from research volunteers. Health questionnaire responses are entered in RVS and queried to identify potential volunteers for participation as research subjects in approved research protocols conducted at NIH. Information from the questionnaire is shared with the NIH research team who may contact volunteers to enroll them in to studies.

The RVS Payment Module is used to process requests for compensation to volunteers by NIH research teams and authorization of payments to research volunteers. The research team provides the SSN as a component of the request for compensation. The requesting research team member's name is stored in the volunteer's record. RVS shares SSN and compensation information with the NIH Business System (NBS) administrative system which tracks expenditures by protocols and NIH Office of Financial Management (OFM) Secure Payee Registration System (SPRS) to process payments to the United States (U.S.) Department of the Treasury.

The RVS stores information that includes volunteer name, date of birth, mailing address, email address, phone numbers, medical record numbers medical information/notes (allergies, current medications, self-reported medical history, sex, right/left hand dominance), and demographic information including, age, race, sex, and NIH clinical research protocol numbers. If selected for

study participation that includes compensation, the NIH IC research team will collect their SSN and enter it into the RVS Payment Module to process payment for their services. RVS also stores the names of NIH staff approving compensation for research volunteers.

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.

Social Security Number
Date of Birth
Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Demographic information, sex
NIH clinical research protocol numbers

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?

The personally identifiable information (PII) in the RVS Contact Management module is used to maintain contact with potential research volunteers and make clinical research volunteer data available to approved or collaborating NIH intramural researchers.

The PII in the RVS Payment Module is used for authorization of compensation by research team members to volunteers participating in approved protocols.

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

Secondary uses of PII are for tracking payments by protocol in a NIH Office of the Director (OD) administrative system, NIH Business System (NBS).

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, 263 and 282.

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 used to cover the system or identify if a SORN is being developed.

09-25-0012, Clinical Research: Candidate Healthy

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Identify the OMB information collection approval number and expiration date

Governmental Sources: 5625-0142-055, Section 2035, exempts research conducted by NIH from Paperwork

Reduction in PRA requirements.

Other Federal Entities

Non-Governmental Sources

Public

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.

None identified.

Describe the procedures for accounting for disclosures.

If a request for an accounting is received, there are audit logs to allow the system administrator to provide that information. Individual components of RVS track functions of logged in users allowing RVS system administrator to account for names of potential research volunteers and date/time the volunteer's health questionnaire was shared with the NIH research team.

Procedures for accounting - will vary from system to system:

If a request for an accounting is received, there are audit logs to allow the system owner to provide that information.

Accounting for disclosures requires both automated and manual processes to compile in systems containing PII. Disclosure to others by the party accessing that information is a manual process, and this may be a formal manual process (tracked with a spreadsheet, for example) or an ad-hoc process (tracked after the fact, only upon request, using information such as notes or emails). There is no one tracking system in place that is in common use for all systems.

The system owner will work with the application administrator to review audit logs to identify persons accessing the requesting individual's information. Tracking the recipient and purpose of PII disclosures to an outside party is a manual process and varies for each application.

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

CC OPR call center staff read the NIH Clinical Center (CC) Research Volunteer System (RVS)

Privacy Notice to potential volunteers and obtain verbal consent from each volunteer before collecting information in RVS. The written privacy notice is also provided by mail to enrolled volunteers. If selected for study participation that includes compensation, the NIH IC research team will collect their SSN and enter it into the RVS Payment Module to process payment for their services.

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 a clinical research trial is voluntary and the collection of PII and medical notes is necessary to conduct NIH research. Therefore, a research volunteer may not opt-out of the collection or use of their PII while participating in clinical research at the CC.

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

Research volunteers are notified of information practices upon first contact with CC OPR call center staff. If there are major system changes that impact the disclosure or use of the volunteers PII, the and the NIH Clinical Center Research Volunteer System Privacy 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 their PII has been inappropriately used or disclosed. The Clinical Center's Privacy Office will review the complaint and respond to the concern within 30 business days. Complaints could also be submitted to the System Manager, who would investigate and share findings with CC Information Systems Security Officer (ISSO) and CC Privacy Officer.

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

Data is reviewed on a regular basis using random checks against source documents and with quality assurance audits by NIH CC Office of Financial Resource Management. I/C principle investigators and research volunteers provide updated contact information and name changes to RVS system administrators. If a research volunteer chooses to leave the program, the RVS Contact Module is updated and the volunteer will not be contacted again.

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 to PII is based on the user's role. Application administrators assign account permissions based on the user's role and current job responsibilities.

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 ICAM 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 use NIH applications must 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).

CC Office of Patient Recruitment staff receive on-the-job training from peers and supervisors.

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 maintained within RVS as required by National Archives and Records Administration (NARA) below.

01-001: Records of All Other Intramural Research Projects
(DAA-0443-2012-0007-0003)

These records span the project life cycle and include, but are not limited to:

Received national or international awards of distinction;

Resulted in a significant improvement in public health, safety, or other vital national interest;

Drew widespread national or international media attention and/or extensive congressional, NIH or other government agency investigation;

Showed the development of new and nationally or internationally significant techniques that are critical for future scientific endeavors; or

Made a significant impact on the development of national or international scientific, political, economic, or social priorities.

Cut off annually at termination of project/program or when no longer needed for scientific reference. Transfer to the National Archives in five year blocks when the newest records in the block are 15 years old.

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.