# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

05/20/2025

### OPDIV:

NIH

### Name:

Clinical Trials Reporting Program

**PIA Unique Identifier:**

P-9160960-546642

**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?**

Yes

**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?**

Existing

**Does the system have Security Authorization (SA)?**

Yes

**Indicate the following reason(s) for updating this PIA.**

Significant System Management Change

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

The system has migrated to a new hosting platform: Cloud1 (aka Cloud One) hosted by the National Cancer Institute using Amazon Web Services.

Additionally, the PII data is de-identified within the system. Meaning that the Privacy Act no longer applies and no PII is shared, internally or externally.

**Describe the purpose of the system.**

The Clinical Trials Reporting Program (CTRP) System is a suite of applications that collect data on trials, protocols, diseases, interventions, patients, people, and organizations; and a Scientific Trials Analytics Platform (STrAP) for viewing, analyzing, comparing, and mining CTRP data.

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

Data is collected on clinical trials, protocols, diseases, interventions, patients, people, and organizations. Potential patient Personally Identifiable Information (PII) is collected and maintained in the System (zip code, date of birth (month/year), sex, demographic information, ICD code/CTEP code). Some of the research information collected and maintained in the System may need to remain confidential due to its proprietary nature. Sensitive research information is collected and maintained in the System.

The CTRP System collects names and email addresses, then uses token-based authentication for access to the system and to confirm permissions/user roles.

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

The Clinical Trials Reporting Program (CTRP) System is a suite of applications that collect data on trials, protocols, diseases, interventions, patients, people, and organizations; and a Scientific Trials Analytics Platform (STrAP) for viewing, analyzing, comparing, and mining CTRP data.

Data is collected on clinical trials, protocols, diseases, interventions, patients, people, and organizations. Potential patient Personally Identifiable Information (PII) is collected and maintained in the System (zip code, date of birth (month/year), sex, demographic information, ICD code/CTEP code). Some of the research information collected and maintained in the System may need to remain confidential due to its proprietary nature. Sensitive research information is collected and maintained in the System.

The CTRP System collects names and email addresses, then uses token-based authentication for access to the system and to confirm permissions/user roles.

**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
patient zip code
patient month and year of birth
patient sex, demographics
patient International Classification of Diseases (ICD) code/Cancer Therapy Evaluation Program (CTEP) code

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

Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Patients

**How many individuals' PII is in the system?**

1,000,000 or more

**For what primary purpose is the PII used?**

The CTRP System uses patient PII to help identify gaps and duplicate studies in clinical research,

facilitates clinical trial prioritization, and standardizes trial data capture and sharing.

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

User name and user email is required for login authentication.

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

Public Health Service Act. (42 U.S.C. 241, 242, 248, 281, 282, 284, 285a-285q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101).

**Are records on the system retrieved by one or more PII data elements?**

No

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

Government Sources

Within the DOC

Non-Governmental Sources

Public

**Identify the OMB information collection approval number and expiration date**

0925-0600, Expiration date 2.28.2026

**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.**

Patient PII is collected from the Principal Investigator or Study Coordinator, and not supplied directly by the study subject. The study subject(aka patient) provides consent to the collection of their personal information when enrolling in the clinical trial.

CTRP users voluntarily provide required login information (PII) when registering to be a user of the application and are provided a link to NCI Privacy and Security policies including the collection of personal 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.**

Patient PII is not collected directly from individuals, but from the Principal Investigator or Study Coordinator. The information required from the individual is agreed upon during the Informed Consent process of enrollment into the clinical trial.

Users of the system provide name and email for login authentication. Access will not be granted without the user's credentials. For CTRP users, there is no opt-out option. Users of the system may decline to give their PII. However, in doing so, they will not be able to access and use the system.

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

NCI has no direct means to identify or contact study subjects/patients whose PII is in the system

because their contact information is not collected. The Principal Investigator and/or Study Coordinator can be notified and then can contact the study subjects/patients whose information is in the system should major changes in disclosure and/or data use change.

**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.**

If individuals patients believe their PII has been inappropriately obtained, used or disclosed, they can file a complaint to the Office of Civil Rights (OCR) within 180 days of the alleged violation. This complaint must be in writing and submitted either by e-mail, postal mail, or fax.

If CTRP users believe their PII has been inappropriately obtained, used or disclosed, they can file a complaint to the NIH Senior Official for Privacy at privacy@mail.nih.gov.

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

The system owner reviews the PII collected in the system on a periodic basis, at least once per year. The NCl requires annual privacy reviews as part of the NIST 800-53 compliance to ensure confidentiality, integrity, and availability of the system and the data maintained within.

**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 granted to those with a direct need to access the data. Access will be granted to non-Federal staff under a non-disclosure agreement and staff will be given mandatory privacy and security training.

The CTRP System uniquely identifies and authenticates all organizational and non-organizational users. Role Based Access Control (RBAC) determines conditions for role/group membership. Permissions sets and groups are defined by the System Owner to ensure least privilege is applied to each role. CTRP System users are only permitted permissions to that of which the role they are assigned.
Roles are reviewed annually by the CTRP System Owner and System Administrator to ensure the principle of least privilege is applied where appropriate.

**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.**

Level of access to PII depends on role and users will be required to undergo security training for their aligned role responsibility. System audit logs facilitate accountability enforcement for user transactions.

The CTRP System uniquely identifies and authenticates all organizational and non-organizational users. Role Based Access Control (RBAC) determines conditions for role/group membership. Permissions sets and groups are defined by the System Owner to ensure least privilege is applied to each role. CTRP System users are only permitted permissions to that of which the role they are assigned.
Roles are reviewed annually by the CTRP System Owner and System Administrator to ensure the principle of least privilege is applied where appropriate.

**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.

**Describe training system users receive (above and beyond general security and privacy awareness training).**

N/A

**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.**

02-004, Extramural program and grants management oversight records. Cut off annually. Destroy 3 years after cutoff (DAA-0443-2013-0004-0004).

07-201, Systems and data security records. Destroy 1 year after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system (DAA-GRS-2013-0006-0001).

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

Administrative Controls: Permission sets and groups are defined by the the NCI System Owner to ensure least privilege is applied to each role. CTRP System users are only permitted permissions to that of which the role they are assigned.
Roles are reviewed annually by the System Owner to ensure they least privilege is applied at an adequate level.

Technical Controls: The CTRP System uses Amazon Web Services (AWS) and Okta Single Sign-on tokens to enforce approved authorizations for logical access to the CTRP System, providing authoritative sources of trusted users and group associations. The CTRP System uniquely identify and authenticate all organizational and non-organizational users. Role Based Access Control (RBAC) determines conditions for role/group membership.

CTRP System NIH Users inherit iTrust implementation of disabling inactive accounts after 60 days of inactivity. For Non-NIH users.

Physical Controls: The CTRP System fully inherits the procedures for implementing physical and environmental security control policies from NCI's CloudOne platform which uses the Federal Risk and Authorization Management Program (FedRAMP) authorized Amazon Web Services. The AWS Infrastructure as a Service (IaaS) East region has a existing FedRAMP Authority to Operate.

**Identify the publicly-available URL:**

https://trials.nci.nih.gov;
https://strap.trials.nci.nih.gov;
https://clinicaltrialsapi.cancer.gov
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