US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/06/2026

OPDIV:

NIH

Name:

NCATS CURE ID

PIA Unique Identifier:

P-5726424-619234

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?

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 NIH National Center for Advancing Translational Science (NCATS) Collaborative Use Repurposing Engine for Infectious Diseases (CURE ID) is a publicly available, collaborative resource for research studies through case reports, references to clinical trials, journal & news articles, events and discussion forums. It hosts a website and mobile application that collects clinical cases on repurposed drugs.

CURE ID is a collaborative partnership between the NCATS and the U.S Food and Drug Administration (FDA).

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

CURE ID collects, hosts, and maintains:
case reports of de-identified electronic health records (EHRs) of patients from hospitals and patient registries that are covered under a Data Transfer & Use Agreement (DTUA),

de-identified information from patients, care partners, and healthcare providers who consent to share this information,
published articles, images of diseases, EHR data extraction guidelines,
Frequently Asked Questions (FAQS), and
user training video that covers the functionality of the platform and published newsletters.

The platform uses data from ClinicalTrials.gov, published articles from PubMed and other journal articles, conferences and webinars, and discussions shared by registered users on the CURE ID platform. CURE ID also hosts and shares narratives of impact stories of drug repurpose experiences of registered and unregistered users who consent to share impact stories. ClinicalTrials.gov and PubMed maintain their own unique privacy impact assessment (PIA) with all legal authorities documented.

The system stores names, email addresses, social sign-on credentials from identity providers, medical qualifications, photos that individuals have consented to share including de-identified images.

Unregistered users are members of the general public who can only browse the CURE ID content.

Registered CURE ID users outside NIH authenticate through Google Cloud Firebase using their email address, social sign-on of identity providers including Apple, Facebook, Google, and X, and password. They are granted access to CURE ID functional services, including the submission of case reports, clinical trials, articles, discussion forums, and events as well as receive notifications of updated CURE ID content. They are allowed to contribute content and participate in discussion forums.

Individuals who support, operate, and maintain the CURE ID system use NCATS Unified NCATS Authentication (NCATS UNA), an identity provider brokering service, which maintains its own unique PIA on record, with all legal authorities documented

NIH users log in to CURE ID using NIH Identity, Credential, and Access Management (IAM) as the identity provider, which maintains its own unique 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.

The system is hosted in Amazon Web Services (AWS) US East/West, which maintains a Federal Risk and Authorization Management Program (FedRAMP) Moderate authorization to operate (ATO), and Google Cloud services, which maintains FedRAMP High Provisional ATO.

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

The NIH NCATS CURE ID is a publicly available, collaborative resource for research studies through case reports, references to clinical trials, journal & news articles, events and discussion forums. It hosts a website and mobile application that collects clinical cases on repurposed drugs.

CURE ID collects, hosts, and maintains:
case reports of de-identified EHRs of patients from hospitals and patient registries that are covered under a DTUA,

de-identified information from patients, care partners, and healthcare providers who consent to share this information,
published articles, images of diseases, EHR data extraction guidelines,
FAQS, and
user training video that covers the functionality of the platform and published newsletters.

The platform uses data from ClinicalTrials.gov, published articles from PubMed and other journal articles, conferences and webinars, and discussions shared by registered users on the CURE ID platform. CURE ID also hosts and shares narratives of impact stories of drug repurpose experiences of registered and unregistered users who consent to share impact stories. ClinicalTrials.gov and PubMed maintain their own unique PIA with all legal authorities documented.

The system stores names, email addresses, social sign-on credentials from identity providers, medical qualifications, photos that individuals have consented to share including de-identified images.

Unregistered users are members of the general public who can only browse the CURE ID content.

Registered CURE ID users outside NIH authenticate through Google Cloud Firebase using their email address, social sign-on of identity providers including Apple, Facebook, Google, and X, and password. They are granted access to CURE ID functional services, including the submission of case reports, clinical trials, articles, discussion forums, and events as well as receive notifications of updated CURE ID content. They are allowed to contribute content and participate in discussion forums.

Individuals who support, operate, and maintain the CURE ID system use NCATS UNA, an identity provider brokering service, which maintains its own unique PIA on record, with all legal authorities documented

NIH users log in to CURE ID using NIH IAM as the identity provider, which maintains its own unique PIA on record, with all legal authorities documented.

CURE ID is a collaborative partnership between the NCATS and the FDA. The system is hosted in Amazon Web Services (AWS) US East/West, which maintains a Federal Risk and Authorization Management Program (FedRAMP) Moderate authority to operate (ATO), and Google Cloud services, which maintains FedRAMP High Provisional ATO.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
Photographic Identifiers
E-Mail Address
Medical qualifications, login credentials for CURE ID account, password
Social sign-in credentials
Consented photographs

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

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

Personally identifiable information (PII) is collected for CURE ID account registration, information dissemination, research and training.

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

NA

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

5 USC 301, Departmental regulations.

42 U.S.C. 241, 242, 248, 281, 282, 284, 285a, 285b, 285c, 285d, 285e, 285f, 285g, 285h, 285i, 285j, 285l, 285m, 285n, 285o, 285p, 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?

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
Government Sources
Other Federal Sources
Non-Governmental Sources
Public
Private Sector

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 following agreements are currently active:
Inter-Agency Agreements (IAA) between NCATS and FDA for the CURE ID program effective through April 30, 2030

Data Transfer and Use Agreements:

NCATS and the Society of Critical Care Medicine
NCATS and the “Count Me In” study

Describe the procedures for accounting for disclosures.

NCATS CURE ID shall maintain an accounting of each disclosure of a record made outside of CURE ID, except for disclosures made under the Freedom of Information Act (FOIA). For each such disclosure, NCATS CURE ID shall record:

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

Individuals are directed to the Privacy Notice on the CURE ID platform which includes a statement that PII is optional and is collected voluntarily.

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.

Users can decline to provide their PII. However, if a user wants to participate and access CURE ID functional services they are required to register and provide their PII.

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

CURE ID has a Privacy Notice which includes a Consent Statement; any changes to the system will be posted in this Privacy Notice. The Privacy Notice is also located on the bottom of the registration and log in pages.

An individual can contact CURE ID support staff via the website and on the mobile app via online email messaging.

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 can communicate concerns to CURE ID support staff on the website and mobile app via on-line email messaging or contact curesupport@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.

NCATS conducts an annual review of PII to ensure integrity, availability, accuracy and relevancy of the data. Approved CURE ID staff will periodically review the PII to ensure that CURE ID accounts have been verified and are active.

Registered users have option to submit a request to delete their data or CURE ID account. This process includes temporarily storing data for 30 days prior to removal.

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 assigned to personnel based upon current job responsibilities and need-to-know basis.

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 access is provisioned based on controls within the system, allowing users only access to the minimum amount of PII 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.

FDA staff that are part of the CURE ID program also have mandatory information technology (IT) Training through the FDA Cybersecurity Awareness Course, which includes: User Responsibility, Protecting Information/Privacy, Threats and Vulnerabilities, Phishing/Social Engineering, Reporting Incidents, Social Media and Networking, Access Control, Remote Access, Portable Devices and Media, Travel Security. Training is completed on the https://fda.csodfed.com with valid FDA credentials.

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

Unregistered users and registered users are provided in-platform walk-through training that covers core functionality and appropriate authorized workflows in the CURE ID system.
Role-Based Training is required for staff designated by NIH as having significant IT security responsibilities. Designated staff are required to complete the following mandatory Role-Based Training Courses: IT Administrator Training and Application Security Checklist & Best Practices for Developers.

All CURE ID staff that are listed on the Institutional Review Board (IRB) protocol for CURE ID's IRB-exempt research study are required to take the appropriate Collaborative IRB Training Initiative (CITI) 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.

01-003, Records of All Other Intramural Research Projects: Records are cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer.
Disposition: Records are destroyed 7 years after cutoff, unless continuation is requested by the Institute, in accordance with the National Archives and Records Administration (NARA) approved disposition schedule: DAA-0443-2012-0007-0003.

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

Administrative:
Access is granted to CURE ID system based on individual roles and responsibilities.
Physical:
The CURE ID system is hosted in Amazon Web Services and Google Cloud Platform, the cloud service providers. These facilities are managed by the cloud service providers.

Technical:
The AWS East/West, a Federal Risk and Authorization Management Program (FedRAMP)-authorized cloud service, and the NCATS Information Technology contract management services of CURE ID ensure that information is secure in the system via several technical means. CURE ID data is encrypted at rest and in transit. Across the hosting platform, management solutions monitor the activities of individuals and services running, the performance of the system resources, and detect security threats.

Identify the publicly-available URL:

https://cure.ncats.io/home

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?

Yes

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

Yes