US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/04/2025

OPDIV:

NIH

Name:

NIDCR CROMS

PIA Unique Identifier:

P-1689542-353289

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 purpose of the National Institute of Dental and Craniofacial Research's (NIDCR) Clinical Research Operations Management System (CROMS) is to store and track studies for clinical research that is funded by the NIDCR extramural and intramural research divisions.

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

The system will collect and store NIDCR staff investigator and study team member names and NIH emails as they appear in the NIH Enterprise Directory (NED) system which maintains its own unique privacy impact assessment (PIA). The system will also collect, and store committee member names and email addresses from outside research institutions or hospitals.

Additionally, the system stores and processes safety event attributes. The following de-identified and anonymous data attributes are collected: date of birth (DOB), demographic information, and medical condition.

Those requiring administrative or infrastructure access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services 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.

Non-NIH users of the application use their home institution's credentials to log into the system. The CROMS system uses single sign on (SSO) functionality to federate with each user's home institution (academic institution/university, or hospital or other research institutions. This allows the CROMS system to delegate authentication.

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

The NIDCR CROMS is used to store and track studies for clinical research that is funded by the NIDCR extramural and intramural research divisions.

The system will collect, and store NIDCR staff. investigator, and study team member names and NIH emails as they appear in the NED system which maintains its own unique PIA. The system will also collect and store committee member names and email addresses along with their outside research institution or hospital name.

Additionally, the system stores and processes safety event attributes. The following de-identified and anonymous data attributes are collected: DOB, sex, demographic information and medical condition are collected.

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.

Non-NIH users of the application use their home institution's credentials to log into the system. The CROMS system uses SSO functionality to federate with each user's home institution (academic institution/university, or hospital or other research institutions.

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

Yes

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

Name
E-Mail Address
De-identified and anonymous DOB, sex, demographic information and medical condition
Name of the outside research institution, hospital or university

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

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

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

PII is used to uniquely identify users of the system.

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

No secondary uses.

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

Section 301 of the Public Health Service Act, (42 U.S.C. 241).

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.

09-25-0216 Administration: NIH Electronic Directory (NED)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A information is not solicited.

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.

NIH staff are made aware during the onboarding process that the information in NED is also used with other applications/systems.

Those outside NIH are provided notice when they log in.

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.

PII is obtained from NED in order to validate the user's identity. If a user opts out of their NED entry, they cannot access the CROM system or other NIH systems.

Individuals outside the NIH can choose to opt out, but then they don't have access to the system.

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

The NIDCR privacy policy page describes collection, sharing and potential use of PII information collected. The CROM website adheres to these standards. There is no additional process in place to notify visitors of any changes to collection of use of PII data provided.

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 may contact the NIDCR Privacy Office through the website's Contact Us page or contact the NIH Privacy Office 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 NIH Information Security Policy Handbook requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all NIDCR systems.

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.

Access to PII is assigned to personnel based upon current job responsibilities. An NIH IAM account login and appropriate permission is required to gain access to the stored data.

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).

All NIDCR staff and direct contract staff are required to take the HHS records management training annually.

Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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 07-203 - System access records. Systems not requiring special accountability for access.

These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
Includes records such as:
user profiles
log-in files
password files
audit trail files and extracts
system usage files
cost-back files used to assess charges for system use

Disposition: Destroy when business use ceases. DAA-GRS-2013-0006-0003

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

Administrative Controls: All technical personnel (federal employees and direct contractors) who access information technology (IT) systems which contain protected information have met background investigation criteria. 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. Access to PII is assigned to personnel based upon current job responsibilities, e.g., role-based access is limited to the nurses and doctors conducting patient data collection and research.

Physical Controls: The 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.

Identify the publicly-available URL:

https://www.nidcrcrms.org/

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