US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/29/2024

OPDIV:

NIH

Name:

NIDCR REDCap

PIA Unique Identifier:

P-2952051-386721

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?

No

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 National Institute of Dental and Craniofacial Research (NIDCR) Research Electronic Data Capture (REDcap) is an easy to use, secure web application for building and managing online databases to support NIDCR research studies. Data pertains to medical research collected under Institutional Review Board (IRB) approved protocols.

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

The primary information collected by the system pertains to medical research data collected under IRB approved clinical protocols to manage these protocols. The data includes, name, mother's maiden name, email address, phone numbers, medical notes, education records, date of birth (DOB), photographic identifiers, mailing address, medical records number (MRN), employment status.

The system also collects NIH Enterprise Directory (NED) identification (ID), name, email address, phone numbers from users (NIH employees and direct contractors) who manage the IRB approved

clinical protocols.

Users log in to this system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique 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 NIDCR REDcap is a secure web application for building and managing online databases to support NIDCR research studies. Data pertains to medical research data collected under IRB approved protocols.

The data collected, maintained and/or shared includes NIH NED ID, name, mother's maiden name, email address, phone numbers, medical notes, education records, DOB, photographic identifiers, mailing address, MRN, employment status. The system collects information on the users of the system who manage the IRB approved clinical protocols. Users may be NIH employees or direct contractors supporting the system.

Users log in to this system using the 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
Photographic Identifiers
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Employment Status
NED ID

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?

500-4,999

For what primary purpose is the PII used?

To facilitate medical research.

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

The data may be used for training and/or research internal to the NIDCR.

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

42 US Code § 241/42 Code of Federal Regulations (CFR) Part 2a

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

09-25-0200, Clinical, Basic and Population-based Research Studies of the NIH

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

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.

Prior to any treatment and collection of data, the study participant signs a protocol consent form with the participant explicitly acknowledging the collection of medical and other data. Any consent form explicitly addresses the use and distribution of the data with respect to confidentiality and the Privacy Act.

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.

Individuals can decline to provide PII. However, submission of PII is a condition to being accepted into any research study, or requests for NIDCR related materials.

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

Users may elect to receive system-generated emails notifying them of major changes and request

consent from individuals whose PII is in the system.

The notification will describe the changes and will give the users the option to remove their data from the database. Without action from the user, the data will remain in the database.

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.

The participant can contact the principal investigator, who will contact the Privacy Officer and/or System Owner for resolution.

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

As a part of the NIH ongoing Assessment & Authorization process, NIDCR performs annual assessments on the management, technical and operational controls which provide for the confidentiality, integrity and availability of the NIDCR RedCAP system.

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. An IAM account login is required to gain access to the stored PII data.

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 rights are 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 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).

Role-based Security Training is required for personnel with significant information security responsibilities to ensure they possess the knowledge and skills needed to protect information and information systems.

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.

Item 03-001 – Clinical Care Service Records

These records document admissions and medical treatment for a patient accepted in a research project. These records are the primary source of evaluation and analysis for either clinical care or clinical research study.

Disposition: Cut off annually at end of fiscal year. Destroy 7 years after cutoff. DAA-0443-2019-0001-0001

Item 03-002 – Radiology and Imaging Records
These records are comprised of X-rays and other roentgenographic images produced by devices and procedures, such as body/head scans created by computerized transaxial tomography (CT). Files may include physician interpretations of images/scans.
Disposition: Cut off in 5 year intervals by fiscal year after file becomes inactive or when no longer needed for clinical reference, whichever is longer. Destroy 60 years after cutoff. DAA-0443-2012-0007-0007

Item 03-005 – Patient Medical Records
These records document admissions and medical treatment for a patient accepted in a research project. These records are the primary source of evaluation and analysis for either clinical care or clinical research study.
Disposition: Cut off annually after medical staff member leaves patient care. Transfer to inactive storage 1 year after cutoff. Destroy 30 years after cutoff. DAA-0443-2012-0007-0011

Item 03-006 – Medical Staff Credentialing Records
These records are comprised of X-rays and other roentgenographic images produced by devices and procedures, such as body/head scans created by computerized transaxial tomography (CT). Files may include physician interpretations of images/scans.
Disposition: Cut off annually after medical staff member leaves patient care. Transfer to inactive storage 1 year after cutoff. Destroy 30 years after cutoff. DAA-0443-2012-0007-0007

Item 03-007 – Pathology Test Records
Pathology test records including media preparation case files, indices and formulas as required by 42 CFR 493. The records contain information related to requisitions for laboratory media and cells, including a description of the method of preparation and the ingredients used.
Disposition: Cut off annually after the date of reporting. Destroy 10 years after cutoff. DAA-0443-2012-0007-0012

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.

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.

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. Virtual Private Network is required for remote access to the system.

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.