US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/31/2024

OPDIV:

NIH

Name:

NIDCR SharePoint

PIA Unique Identifier:

P-9526920-927597

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?

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 system was using the no longer available NIH-wide Contact Info privacy impact assessment (PIA) to account for personally identifiable data. The system now accounts for it.

Describe the purpose of the system.

The National Institute of Dental and Craniofacial Research (NIDCR) SharePoint Intranet site is used as a document repository and collaboration portal for NIDCR. It is also used to manage several internal business applications using forms and workflows.

Microsoft SharePoint collaboration software provides automated workflow management and document repository/storage for NIDCR offices and divisions.

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

The primary information type collected, maintained and stored is administrative, technical and management program data. This includes the following data: information technology (IT)

management, planning and budgeting, training and development, research and development, post-award grant, and intellectual property protections. This data is used as an aid for NIDCR research or administrative purposes, to support business processes and operations, and does contain personally identifiable information (PII) from the NIH Enterprise Directory (NED). Data includes name, NIH email address, date of birth (DOB), phone numbers, and photographic identifiers. Device identifiers are also collected.

NIDCR staff access this site using the NIH Identity, Credential, and Access Management (IAM) Services . The purpose of the IAM 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 collects unique user names and passwords (user credentials) and stores them in an encrypted format. The IAM is an essential service which facilitates and governs network access to various resources.

NED and NIH IAM Services maintain their own unique privacy impact assessment (PIA), with all legal authorities documented.

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

The NIDCR SharePoint Intranet site is used as a document repository and collaboration portal for NIDCR. It is also used to manage several internal business applications using forms and workflows.

Microsoft SharePoint collaboration software provides automated workflow management and document repository/storage for NIDCR offices and divisions.

The primary information type collected, maintained and stored is administrative, technical and management program data. This includes the following data: IT management, planning and budgeting, training and development, research and development, post-award grant, and intellectual property protections. This data is used as an aid for NIDCR research or administrative purposes, to support business processes and operations, and does contain PII from NED. Data includes name, NIH email address, DOB, phone numbers, and photographic identifiers. Device identifiers are also collected.

NIDCR staff access this site using the NIH IAM Services.

NED and NIH IAM Services maintain their own PIA, 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.

Date of Birth
Name
Photographic Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Device Identifiers
IT management data, planning and budgeting data, training and development data, research and development data, post-award grant data, and intellectual property protections.

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?

500-4,999

For what primary purpose is the PII used?

The data is used to facilitate the dental and craniofacial research related to the NIDCR mission.

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

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

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.

Employees are notified prior to obtaining access to any NIDCR system - including the NIH SharePoint system - that PII may collected.

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.

There is no option to opt-out of the collection or use of PII. NIDCR SharePoint users have already provided consent to provide PII as a part of employment or use of the system via NIH NED. Any additional PII is required to be submitted such as contact information when filling out a form.

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

Individuals will be contacted using the contact information (email or phone number) in the system. If necessary, they would be asked to re-consent to any changes.

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 Coordinator for resolution, or contact the NIH Privacy Office at Privacy@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.

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 SharePoint system. The NIDCR Privacy Coordinator, along the with the system owner, perform annual activities, including, but not limited to:
Review and/or updates to the NIDCR PIA and risk assessment,
Review of NIH privacy requirements, including mandatory privacy awareness & training
Review and/or updates of NIH procedures for accounting for privacy disclosures
Conduct analysis and review for the minimization of PII
Review data retention requirements and disposal methods
Review and update procedures for individual consent, redress and complaint management
Review Use Limitation for authorized uses of collected data
Validate inventory of PII
Review NIH Privacy Incident Response Plan and standard operating procedures

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 and use of these records is limited to those persons whose official duties require such access. Access is granted by System Administrators following approval by System Owners and/or approved Principal Investigators. 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.

Users are assigned to specific roles which limit the information available to them to perform their duties.

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).

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 07-204 - System access records. Systems 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.
Disposition: Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. DAA-GRS-2013-0006-0004

Item 07-201 – Systems and data security records
These are records related to maintaining the security of information technology (IT) systems and data.
Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific
systems for which they were written. This series also includes analysis of security policies, processes, and
guidelines, as well as system risk management and vulnerability analyses.
Disposition: Destroy 1 year(s) 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

Item 7-102 Information technology development project records. Infrastructure project records.
Information Technology infrastructure, systems, and services project records document the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications.
Disposition: Destroy records 5 years after project is terminated, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS-2013-0005-0006.

Item 07-103 Information technology development project records. System development records.
These records relate to the development of IT systems and software applications through their initial stages up until hand-off to production which includes planning, requirements analysis, design, verification and testing, procurement, and installation. Records include case files containing documentation of planning, decision making, designing, programming, testing, evaluation, and problem solving.
Disposition: Destroy records 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS-2013-0005-0007.

Item 07-105 Information technology operations and maintenance records.
Relates to the activities associated with the operations and maintenance of the basic systems and services used to supply the agency and its staff with access to computers and data tele-communications. Includes the activities associated with IT equipment, IT systems, and storage media, IT system performance testing, asset and configuration management, change management, and maintenance on network infrastructure.
Disposition: Destroy records 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS-2013-0005-0004.

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 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.