US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/17/2024

OPDIV:

NIH

Name:

NIDCR GSS: NIDCR Internet Website (Acquia)

PIA Unique Identifier:

P-2926801-549231

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?

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 is now Agency operated. No other changes have occurred since the last assessment.

Describe the purpose of the system.

The purpose of this system is to provide a portal for the National Institute of Dental and Craniofacial Research (NIDCR) to communicate information topics to the public. This is the primary public-facing, internet website for NIDCR and includes the posting and dissemination of information relating to the various research topics being studied by the NIDCR.

The site is hosted in the Acquia Cloud Enterprise (ACE) Platform as a Service (PaaS) for general computing purposes and the hosting of the public website(s).

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

Information suitable for public distribution and related to the research and mission of the NIDCR is posted to the website.

The system also stores the names, email addresses, phone numbers and photographic identifiers of members of the public who may collaborate on research with NIDCR or request additional information. The same information is posted for NIDCR staff members in support of their job functions to further the NIDCR mission. Employee information originates from NIH Enterprise Directory - NED, the source system.

Those requiring administrative access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (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.

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

The purpose of this system is to provide a portal for the NIDCR to communicate information topics to the public. This is the primary public-facing, internet website for NIDCR and includes the posting and dissemination of information relating to the various research topics being studied by the NIDCR.

The site is hosted in the ACE PaaS for general computing purposes and the hosting of the public website(s).

Information suitable for public distribution and related to the research and mission of the NIDCR is posted to the website.

The system also collects, maintains and stores the names, email addresses, phone numbers and photographic identifiers of members of the public who may collaborate on research with NIDCR or request additional information.

The same information is posted for NIDCR staff members in support of their job functions to further the NIDCR mission. Employee information originates from NIH Enterprise Directory - NED, the source system.

Those requiring administrative access to this system log in using the NIH IAM Services which maintains its own unique PIA on record, 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.

Name
Photographic Identifiers
E-Mail Address
Phone Numbers

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

Employees

Public Citizens

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

PII is used to contact NIDCR staff and collaborators.

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.

Public Health Service Act, 42 USC § 203, 241, 285c; 44 USC § 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.

09-25-0216 Administration: NIH Electronic Directory

09-90-1901 HHS Correspondence, Comment, Customer Service, and Contact List Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Email

Online

Government Sources

Within OpDiv

NIH

Non-Government Sources

Public

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

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.

NIDCR employees are notified at the time of hire that non sensitive personally identifiable information (PII) can be collected, maintained and/or shared.

External users voluntarily provide PII if they wish to get more information or contact someone within NIDCR.

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 have a right to not give their PII, however, that would preclude them from getting more information.

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

Individuals would 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.

Periodic audits are conducted (at least once a year) by authorized users to ensure the data's integrity, availability, accuracy, and relevancy.

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 using 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 function.

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 IAM account login is required to gain access to the stored PII 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. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). 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 7-102 Information technology development project records. Infrastructure project records. Information Technology (IT) 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.

Identify the publicly-available URL:

www.nidcr.nih.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?

Yes

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

Yes