US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/08/2024

OPDIV:

NIH

Name:

NIDCR NOHIC

PIA Unique Identifier:

P-2025470-503488

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.

Contractor

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.

Migration to the Microsoft (MS) Azure cloud environment.

Describe the purpose of the system.

The National Institute of Dental and Craniofacial Research (NIDCR) established the National Oral Health Information Clearinghouse (NOHIC) with the mission of providing a single, centralized source of information and publications- for professionals, patients, and the public- on special care in oral health.

The primary functions of NOHIC include the following:
Respond to inquiries and distribute information and materials.
Develop materials including fact sheets, directories, and brochures.
Perform outreach and promotion activities, including networking and coordination, within the field of special care in oral health.

Users may select and order a variety of free publications from the website.

NOHIC, operated under contract to NIDCR, is a program arm of NIDCR's Office of Communications and Health Education (OCHE).

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

In order to provide the requested information, the site collects Name, Email address, mailing address, telephone number, profession and where the information will be used (Doctors office, clinic, etc.). Users may select and order a variety of free publications from the website.

Those requiring access to administer 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 NIDCR established the NOHIC with the mission of providing a single, centralized source of information and publications-for professionals, patients, and the public-on special care in oral health.

The primary functions of NOHIC include the following:
Respond to inquiries and distribute information and materials.
Develop materials including fact sheets, directories, and brochures.
Perform outreach and promotion activities, including networking and coordination, within the field of special care in oral health.

In order to provide the requested information, the site collects Name, Email address, mailing address, telephone number, profession and where the information will be used (school, clinic, etc.). Users may select and order a variety of free publications from the website.

Those requiring access to administer this system log in using the NIH IAM Services which maintains its own unique PIA on record, with all legal authorities documented.

NOHIC, operated under contract to NIDCR, is a program arm of NIDCR's OCHE.

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
Mailing Address
Phone Numbers
Profession
Where materials will be used

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

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The information collected is used to send materials to end users who request it.

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

There are no secondary uses of personally identifiable information (PII).

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

The legal authority to operate and maintain this Privacy Act records system is 42 U.S.C. §§ 241, 248, 282 and 284; E.O. 13478, Executive Order 9397 (8 Fed. Reg. 16,094), as amended. by, Executive Order 13478 (73 Fed. Reg. 70,239.

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.

09-25-0106, “Administration: Office of the NIH Director and Institute/Center Correspondence

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Non-Governmental Sources
Private Sector

Identify the OMB information collection approval number and expiration date

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

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.

The page footer on catalog.nidcr.nih.gov provides information regarding authority to collect information as well as use of collected information. In addition, there is a link and references to NIDCR Privacy Policy page. There are no additional processes in place to notify visitors of any changes to collection or use of PII data provided.

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 collected on voluntary basis and only for purposes of shipping desired publications to the requester. Users may opt out by not ordering any publications.

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

When a user navigates to the catalog.nidcr.nih.gov, the page footer contains link and references to NIDCR Privacy Policy page. The NIDCR privacy policy page describes collection, sharing and potential use of PII information collected. The catalog.nidcr.nih.gov website adheres to these standards. There are 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 Contact Us page or contact the NIH Privacy office of 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.

Records are kept during the year to validate and confirm the order status and ship date for a customer.

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 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).

All NIDCR 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 10-102 Non-recordkeeping copies of electronic records.
Non-recordkeeping copies of electronic records. Non-recordkeeping copies of electronic records agencies maintain in email systems, computer hard drives or networks, web servers, or other locations after agencies copy the records to a recordkeeping system or otherwise preserve the recordkeeping version.
Disposition: Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use. DAA-GRS-2016-0016-0002

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 information technology (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://catalog.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