US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/05/2025

OPDIV:

NIH

Name:

DPCPSI Website

PIA Unique Identifier:

P-8429303-623266

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?

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.

Updated to Drupal to provide specific permissions to only allow administrators to view the list of users.

Describe the purpose of the system.

The Division of Program Coordination, Planning, and Strategic Initiatives (DPCPSI) website DPCPSI.nih.gov disseminates information about the Division to the public and to National Institutes of Health (NIH) staff. It also provides NIH staff with guidance and other helpful materials for training, tools, consultation, planning and supporting challenges and prize competitions.

DPCPSI includes an intranet site for Drupal, which is not part of the system. Drupal maintains its own unique Privacy Impact Assessment (PIA).

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

The system stores public program information. It has a webform component which can be used to collect information but is not used to collect personally identifiable information (PII) or sensitive data.

The specific data elements being stored and shared are HyperText Markup Language (HTML) formatted text, supporting documents (such as Portable Document Format (PDF), Word, Excel, etc.) and images.

Some offices in the DPCPSI site have staff pages which display name, email address, phone number, mailing address, title and/or organization, and sometimes head shots for office staff. This information is collected either directly from individuals through voluntary submissions (e.g., online forms or email correspondence) or derived from the NIH Enterprise Directory (NED), an electronic directory and the authoritative source for identity management at NIH. Information from NED is provided by the individual as part of the hiring process and supports electronic government and administrative business processes at NIH. NED has its own unique PIA.

The system stores user's (content editor and administrator) username and email address. Those accessing DPCPSI with this specific contact information, log in using the NIH Identity, Credential, and Access Management (IAM) Services, which maintains its own unique PIA. 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 usernames 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.

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

DPCPSI website DPCPSI.nih.gov disseminates information about the Division to the public and to NIH staff. It also provides NIH staff with guidance and other helpful materials for training, tools, consultation, planning and supporting challenges and prize competitions.
DPCPSI includes an intranet site for Drupal, which is not part of the system. Drupal maintains its own unique PIA.

The system stores public program information. It has a webform component which can be used to collect information but is not used to collect PII or sensitive data. The specific data elements being stored and shared are HTML formatted text, supporting documents (such as PDF, Word, Excel, etc.) and images.

Some offices in the DPCPSI site have staff pages which display name, email address, phone number, mailing address, title and/or organization, and sometimes head shots for office staff. This information is collected either directly from individuals through voluntary submissions (e.g., online forms or email correspondence) or derived from the NIH NED, an electronic directory and the authoritative source for identity management at NIH. Information from NED is provided by the individual as part of the hiring process and supports electronic government and administrative business processes at NIH. NED has its own unique PIA.

The system stores user's (content editor and administrator) username and email address. Those accessing DPCPSI with this specific contact information, log in using the NIH IAM Services, which maintains its own unique PIA. 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 usernames 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.

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
Mailing Address
Phone Numbers
Title and/or organization

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The primary purpose for the PII is to manage DPCPSI correspondence, information dissemination, and customer service functions.

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

N/A

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

42 U.S. Code § 282 - Director of National Institutes of Health; 5 U.S.C. 301, 302, 305, 553; 21 U.S. C. 301 et seq.; 31 U.S.C. 1115(b)(6); 40 U.S.C. 11313; 42 U.S.C. 201 et seq.; 44 U.S.C. 3101, 1505; E.O. 11583; E.O. 13571

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, 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
Non-Government Sources
Public
Commercial Data Broker
Media/Internet
Private Sector

Identify the OMB information collection approval number and expiration date

N/A. Cited in Office of Management and Budget's (OMB) Open Government Directive on Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act (April 7, 2010). The system does not solicit information from members of the public.

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.

Individuals are directed to the NIH Privacy Policy which includes a statement indicating that the provision of PII is optional and collected voluntarily.

Employees are notified during the on-boarding process that their contact information and picture are available in a directory. They may contact Human Resources (HR) if they need assistance.

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.

The collection of contact information is voluntary. However, failure to do so may delay or prevent further communication.

As an electronic directory supporting e-government and administrative business processes, the information is obtained from NED, the source system and maintains its own PIA.

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

There are no foreseen major changes to the handling of PII that may affect privacy risk. Should any of the systems modify the way its data is used or disclosed, an appropriate option for notifying individuals and obtaining their consent will be employed.

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.

Should concerns arise or a need to update information, individuals may access the "Contact Us" page of the website or 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 technology (IT) Privacy Program 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 systems, networks and interconnected systems.

Regular security, 'health checks' and backups are completed, and any vulnerabilities are addressed. PII is generally collected as a one-time use in a request for additional information on a particular topic or application.

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.

There is no opt-out for system administrators. If system administrators don't want to enter their credentials, then they aren't able to access the system to perform their duties.

Direct contractors may have access to this information in order to provide a response. These direct contractors are held to strict policies to safeguard the information and provide the same level of privacy protection as guaranteed by NIH.

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.

Only those individuals with need-to-know are given access to the permissions-based system. 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.

Those accessing information log in using the NIH IAM Services which maintains its own unique PIA.

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 information security and information management 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).

Content management system (CMS) training is available for users (content editors).

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 11-202 - Public Correspondence and Communications not Requiring Formal Action.
Records related to correspondence and communications, including comments, to and from the public that require no formal response or action.
Disposition: Destroy when 90 days old, but longer retention is authorized if required for business use.
DAA-GRS-2016-0005-0002

Item 07-105 - Information technology operations and maintenance records.
Records related to website administration, code, templates, style sheets, site architecture, change requests, site postings. Any activities with a major impact to the system are maintained as part of RSS Item 07-106 (Configuration and Change Management Records).
Disposition: Destroy 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.

DAA-GRS-2013-0005-0004

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

12-039 - Administration: NIH Enterprise Directory (HHS/NIH)
This system allows for the creation of accurate records for individuals in the NIH directory and ensures that duplicate data files are compared, corrected, and combined for accuracy, thus, eliminating redundancy. It is the central point of coordination for other automated systems that manage or track resources, particularly information security systems.
Disposition: Destroy when business use ceases.
DAA-GRS-2016-0016-0001

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

Actual contact information is managed by the NIH Office of the Director (OD), or the NIH Center for Information Technology (CIT), and follow security procedures to secure the platform, and all PII retained , using administrative, technical, and physical controls. Permissions are in place by the Institute or Center (ICO) to limit access to those who need to act on the data provided.

Physical controls: The website is hosted on Acquia Cloud which utilizes an Amazon Web Services (AWS) platform. Amazon's AWS data centers follow and enhance best practices in data center physical security. The exterior physical security is military grade. Personnel who enter the data center are authorized and verified by a government issued identification (ID), and two-factor authentication at each entrance point. Each entrance is monitored by video surveillance, and Amazon logs and audits all access. All visitors and contractors must present identification and sign in. Visitors are always escorted by authorized staff. Amazon AWS does not permit guests, subscribers, or strategic partners such as Acquia to either tour or inspect its data center. Therefore, Acquia can't facilitate any physical inspection of AWS hosting facilities for subscribers.

Acquia maintains some infrastructure on its premises—for example, Internet Protocol (IP) phone switches and Local Area Network (LAN) equipment. This equipment isn't used either to host subscriber applications or to store sensitive subscriber information.

Technical controls include User ID, passwords, network firewall, Virtual Private Network (VPN), Intrusion Detection System, Role Based Access Controls, System logs. 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 authentications must be used for access. File integrity and auditing software are employed on hardware.

Administrative controls include system security and contingency plans. Files are backed up regularly. All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these sites use privileged and separate accounts for administrative access.

More information about Acquia Security Controls and Physical Security can be found here: https:

//docs.acquia.com/acquia-cloud-platform/architecture/security

Identify the publicly-available URL:

https://dpcpsi.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