US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/28/2024

OPDIV:

NIH

Name:

NIBIB Contact Info

PIA Unique Identifier:

P-2052162-842283

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?

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 Biomedical Imaging and Bioengineering (NIBIB) maintains applications and/or websites that collect basic contact information to respond to unsolicited requests for information and/or to provide directory services.

The NIBIB Contact Info privacy impact assessment (PIA) is intended as an umbrella assessment and covers the following systems:
NIBIB Magnetic Resonance Imaging (MRI Atlases)
NIBIB Public Website

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

The NIBIB Contact Info can collect the following data elements: name, email address, phone number, mailing address, photographic identifier, title and/or organization.

There are only two use cases when NIBIB Contact Info can be leveraged:
When collecting data that is derived from a “Contact us” type of form, such as those on a public facing website, or -
As an electronic directory supporting e-government and administrative business processes at NIH. (The minimum personally identifiable information (PII) is publicly available on the public facing NIH NED and is required as part of the hiring process).

Each system leveraging NIBIB Contact info will include:
Specific data elements leveraged
Number of users that could be affected
Applicable System of Record Notice (SORN)

Contact Info can collect name, email address, phone number, mailing address, photographic identifier, title and/or organization.

Those requiring access to process requests log in using the NIH Identity , Credential, and Access Management (IAM) Services, which maintains its own unique privacy impact assessment (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 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 maintains its own unique PIA on file, 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 National Institute of Biomedical Imaging and Bioengineering (NIBIB) maintains applications and/or websites that collect basic contact information to respond to unsolicited requests for information and/or to provide directory services.

The NIBIB Contact Info privacy impact assessment (PIA) is intended as an umbrella assessment and covers the following systems:
NIBIB Magnetic Resonance Imaging (MRI Atlases)
NIBIB Public Website

The NIBIB Contact Info can collect the following data elements: name, email address, phone number, mailing address, photographic identifier, title and/or organization.

There are only two use cases when NIBIB Contact Info can be leveraged:
When collecting data that is derived from a “Contact us” type of form, such as those on a public facing website, or -
As an electronic directory supporting e-government and administrative business processes at NIH. (The minimum PII is publicly available on the public facing NIH NED and is required as part of the hiring process).

Each system leveraging NIBIB Contact info will include:
Specific data elements leveraged
Number of users that could be affected
Applicable SORN

Contact Info can collect name, email address, phone number, mailing address, photographic identifier, title and/or organization.

Those requiring access to process requests log in using the NIH IAM Services, which maintains its own unique PIA.

NED maintains its own unique PIA on file, 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
Mailing Address
Phone Numbers
Title, 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
Patients

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

To contact or register an individual.

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.

5 U.S.C. 301, 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, 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

Non-Government Sources

Public

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

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 NIBIB's Privacy Policy/Notice which includes a statement that personally identifiable information (PII) is optional and is 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.

Users can decline to provide PII. However, without their contact information there is no way to respond directly.

As an electronic directory supporting e-government and administrative business processes, the information is obtained from NED, the source system. NED 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 will be no substantive changes to data uses. Information is collected in order to respond to requesters. There is no further use of PII. In the event of a major change, the email address will be used to contact individuals.

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

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.

If an individual chooses to include personal information, it is voluntary. Should concerns arise or a need to update information, users could access the "Contact Us" page of the site or the NIH Privacy Office at Privacy@mail.nih.gov.

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

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 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.

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

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.

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

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 information security and information management training. There are five categories of mandatory 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.

Content management system (CMS) training is available for users of specific NIBIB systems. This may be SharePoint, Drupal or other.

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 11-102 - 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 07-203 - System access records. Systems not requiring special accountability for access.
System access records.
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.

Physical controls may include 24x7 guards, secure building access, Personal Identify Verification (PIV) card access and/or closed-circuit TV. 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 include User identification (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.

Identify the publicly-available URL:

https://nibib.nih.gov
https://www.imagwiki.nibib.nih.gov

Available to the public with authorization:
https://tgm.nibib.nih.gov/
https://tortoise.nibib.nih.gov/
https://sedfitsedphat.nibib.nih.gov/default.aspx
https://nih.sharepoint.com/sites/NIBIB-SPP
https://nih.sharepoint.com/sites/NIH-MDRIG/SitePages/Home.aspx

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