US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/31/2024

OPDIV:

NIH

Name:

NIH Freedom of Information Act Program

PIA Unique Identifier:

P-7586620-980645

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

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.

There have been no substantial changes to the system.

Describe the purpose of the system.

The NIH Freedom of Information Act Program (NIH FOIA) is a centralized platform for individuals to exercise their right to access information held by the NIH under the provisions of FOIA. By streamlining the processing of FOIA requests, the system promotes transparency and accountability within NIH.

The publicly accessible site allows users to submit FOIA requests and receive final released documents electronically, provides tools for users to track the status of their request, facilitates communication between requesters and the NIH staff, and offers educational resources about the FOIA process, including requester rights, NIH policies and procedures, and tips for submitting effective FOIA requests.

The system also allows personnel to securely store, process (redact), and transmit responsive records, and generate associated correspondence and internal and public reports in a manner that complies with statutory and Department of Justice requirements and best practices.

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

The information typically entered into FOIA includes the requester's name, contact information, and a description of the records requested. The type of contact information included in the system depends on the contact information provided by the requester, which may include the requester's name and an email, work, or home address, mobile, work, and/or home phone, job title, and/or organization or entity name.

All records related to the processing of a request are also uploaded into FOIA. The type of records uploaded include the original FOIA request, all records responsive to the request including the original, working drafts with redactions marked and reviewers' comments, and redacted versions.

Documents that are provided to fulfill FOIA request may have any form of PII. All PII in these documents are collected by the FOIA system then redacted before information is shared with the requester.

The system contains personally identifiable information pertaining to the requester as well as about other individuals who may be referenced in documents responsive to a particular request.

Individual and entity requesters may submit requests through various communications methods including Public Access Link (PAL) Portal (Primary), U.S. mail, or e-mail. Requests may also be received by referral from another federal FOIA office.

External users (the public) login into the Public Access Link (PAL) module of FOIAXpress using the username and password that they created when setting up their account.

NIH FOIA staff access the system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including 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 collect unique user credentials and stores them in an encrypted format. The IAM Services are 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 NIH Freedom of Information Act Program (NIH FOIA) is a centralized platform for individuals to exercise their right to access information held by the NIH under the provisions of FOIA. By streamlining the processing of FOIA requests, the system promotes transparency and accountability within NIH.

The publicly accessible site allows users to submit FOIA requests and receive final released documents electronically, provides tools for users to track the status of their request, facilitates communication between requesters and the NIH staff, and offers educational resources about the FOIA process, including requester rights, NIH policies and procedures, and tips for submitting effective FOIA requests.

The system also allows personnel to securely store, process (redact), and transmit responsive records, and generate associated correspondence and internal and public reports in a manner that complies with statutory and Department of Justice requirements and best practices.

The information typically entered into FOIA includes the requester's name, contact information, and a description of the records requested. The type of contact information included in the system depends on the contact information provided by the requester, which may include the requester's name and an email, work, or home address, mobile, work, and/or home phone, job title, and/or organization or entity name.

All records related to the processing of a request are also uploaded into FOIA. The type of records uploaded include the original FOIA request, all records responsive to the request including the original, working drafts with redactions marked and reviewers' comments, and redacted versions.

Documents that are provided to fulfill FOIA request may have any form of PII. All PII in these documents are collected by the FOIA system then redacted before information is shared with the requester.

Individual and entity requesters may submit requests through various communications methods including Public Access Link (PAL) Portal (Primary), U.S. mail, or e-mail. Although. Requests may also be received by referral from another federal FOIA office.

External users (the public) login into the Public Access Link (PAL) module of FOIAXpress using the username and password that they created when setting up their account.
NIH FOIA staff access the system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including 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 collect unique user credentials and stores them in an encrypted format. The IAM Services are 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.

Social Security Number
Date of Birth
Name
Photographic Identifiers
Driver's License Number
Biometric Identifiers
Mother's Maiden Name
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Certificates
Legal Documents
Education Records
Device Identifiers
Military Status
Employment Status
Foreign Activities

Passport Number
Taxpayer ID
user name and password
organization and job title

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?

10,000-49,999

For what primary purpose is the PII used?

The primary purposes for which personally identifiable information (PII) is used are to create user accounts in the NIH FOIA Request Portal; to track, process, and respond to requests; and to verify the identity of individual requesters.

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

Not Applicable

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

5 U.S.C. 552, 552a; 44 U.S.C. 3301.

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.

09-90-0058 Tracking Records and Case Files for FOIA and Privacy Act Requests and Appeals

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Hardcopy
Email
Online
Government Sources
Within the Agency
Other HHS Agency
State/Local/Tribal
Non-Governmental Sources
Public

Identify the OMB information collection approval number and expiration date

N/A. The request mechanism does not constitute an information collection under 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 visiting the NIH FOIA website are provided a Privacy Act Statement informing them of the collection of their personal information.

This Statement is provided pursuant to the Privacy Act of 1974 (5 U.S.C. § 552a): The information you are requested to provide in order to use the NIH FOIA Request Portal is authorized to be collected under the Freedom of Information Act (5 U.S.C. § 552). Completing the request portal fields is voluntary, but failing to provide any or all of the requested information may prevent HHS from creating a portal account for you, or may prevent HHS from processing your request. The principal purposes for which HHS will use the information that you provide in the NIH FOIA Request Portal are to create an account for you, and to track, process, and respond to requests that you submit to HHS through your account. The information you provide will be included in a Privacy Act system of records, and will be used and may be disclosed for the purposes and routine uses described and published in the following System of Records Notice (SORN): 09-90-0058 Tracking Records and Case Files for FOIA and Privacy Act Requests and Appeals https://www.federalregister.gov/articles/2016/03/29/2016-07060/privacy-act-of-1974-system-of-records-notice

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.

Completing the request portal fields is voluntary and individuals have the right to not submit their personally identifiable information (PII). However, failing to provide any or all of the requested information may prevent NIH FOIA from creating a portal account or processing your request.

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

Upon any major system change, all NIH FOIA staff and FOIA requesters will be made aware through an update to the NIH FOIA public facing website advertising the change to the system.

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.

An individual's concern that his/her PII was inappropriately released by the NIH FOIA program would be reported by said individual to the NIH FOIA officer utilizing the contact information published on the NIH FOIA public facing website. The NIH FOIA Officer will work directly with the NIH Privacy Office to handle any PII related issue as necessary. NIH and HHS will handle privacy incidents by analyzing said inquiry to determine if an improper disclosure occurred; the concern would be responded to in writing; and remedial measures would be taken if an improper disclosure occurred.

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 system administrator periodically reviews all content, including PII for data 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 on role-based access controls and the principle of 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. NIH FOIA personnel are required to login using NIH IAM Services before they can access 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 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).

Because the users are information disclosure specialists, they receive specialized training on a regular basis at FOIA/PAL(Public Access Link) conferences and workshops hosted by HHS, the Department of Justice, and outside vendors providing advanced instructions and guidance regarding safeguarding personal privacy information and avoiding improper disclosures of PII in particular contexts and with respect to specific types of records.

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 following NIH Records Retention Schedule:

Item 08-203. Access and disclosure request files. -
Case files created in response to requests for information under the Freedom of Information Act (FOIA), Mandatory Declassification Review (MDR) process, Privacy Act (PA), Classification Challenge, and similar access programs. Disposition: Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use.
Disposition: DAA-GRS-2016-0002-0001

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

Administrative: The system conducts or performs management oversight activities, security awareness and training, separation of duties for personnel administering the system. In addition, all personnel with access to the system are required to abide by the HHS and NIH Rules of Behavior upon completing security awareness training as a new hire and then annually. Requirements for accounts to the back end of the FOIA system include NIH background check, having a valid need-to-know , and a separation of duties structure which ensures that no single individual role has control of any critical process in its entirety. User access is limited based on role and are controlled by the System Admin, who uses the admin tool to download, maintain and monitor access, including passwords and user names. Accounts are fully deactivated when personnel transition.

Technical: Records stored in the system are protected by Opexus and Deloitte in their approved Federal Risk and Authorization Management Program (FedRAMP) Moderate authorized environments through the use of Transport Layer Security (TLS) 1.2 and Federal Information Processing Standard Publication (FIPS) 140-2 compliant encryption.

Physical: The NIH FOIA system is entirely hosted within the Opexus and Deloitte FedRAMP Moderate authorized environments. The system infrastructure components are maintained withinFedRAMP certified environments, and physical security controls are inherited under the Opexus and Deloitte's shared responsibility model through the use of CCTV's, physical security staff, Biometric ID Badging to respective environments, and biometric turn-styles.

Identify the publicly-available URL:

https://foiaportal.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?

No

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

null