US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/18/2025

OPDIV:

NIH

Name:

NHLBI Public Website System (PWS)

PIA Unique Identifier:

P-9367149-604680

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?

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 Heart, Lung, and Blood Institute (NHLBI) Public Website System (PWS) is the main communication tool used to provide health education to the public related to heart, lung and blood research and news. NHLBI uses the site to inform the public about its mission, vision, organization, events, and programs. In addition, the website is used for community and social services; public services; and to meet the open government requirement. There are two main parts of the NHLBI PWS: the public-facing site that presents NHLBI mission and other education materials to the general public, and the internal-facing site that allows for maintenance of content, as well as access to tools and services.

The public-facing website includes the following distinct interfaces: National Institutes of Health (NIH) Centers for Accelerated Innovations - Research Evaluation and Commercialization Hubs (NCAI-Reach) microsite, Aim for a Healthy Weight Body Mass Index (BMI) Calculator, Community Health Workers, We Can!, Chronic Obstructive Pulmonary Disease (COPD) National Action Plan (CNAP) Community Action Tool, Trans-Omics for Precision Medicine (TOPMed) Program Website, Genome-

Wide Repository of Associations Between Single Nucleotide Polymorphisms (SNP) and Phenotypes (GRASP) search tool, Developmental Biology, and Healthy Eating microsite.

The internal-facing website includes the following interfaces: Division of Intramural Research (DIR) Web Services, NHLBI Digital Asset Management (DAM) system and Data Analytics Metric Dashboard.

External links to Archive-It.org and GovDelivery.com may collect personally identifiable information (PII), which is handled by the third parties. NHLBI is working on a Third-Party Website Applications (TPWA) for those two systems.

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

The NHLBI PWS maintains and shares information about NHLBI Executive and Division Leadership team, including name, photo, email, staff biography, and position title. The NHLBI PWS maintains and shares information about NHLBI Divisions, including email, phone number, and address.

Contact page maintains mailing address and includes a link to the NIH Enterprise Directory (NED) that maintains its own unique Privacy Impact Assessment (PIA) with all legal authorities documented.

Visitors non-sensitive data regarding portal visit is also collected, which includes: computer Internet Protocol (IP) address, domain, website's Internet address, product and version of the visitor's operating system and browser, date and time the visitor arrived and how long the visitor spent visiting the site (which links/features/pages they clicked/accessed).

The following interfaces collect PII to create an account, and provide a link to access those accounts by 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.

NCAI-Reach microsite collects email, username, password and organization for account creation.

CNAP Community Action Tool microsite collects email, username, password and organization.

Developmental Biology microsite collects name, email and phone number.

Healthy Eating microsite collects email and password.

Aim for a Healthy Weight microsite's BMI Calculator page collects height and weight.

We Can! microsite collects email and comments.

GRASP search tool microsite collects visitor's name, email, study title, publication date, study subject's ancestry

TOPMed Program Website collects name, email, professional title, phone number, fax number, degree, organization, department, address, city, state, zip code, country, study title, publication date, username and password.

DIR Web Services collects name, email, phone numbers and laboratory name.

NHLBI DAM system maintains media assets, including images, video, PDF documents, email and phone numbers.

Data Analytics Metric Dashboard collects email and password.

Adobe Analytics collects web metrics information about visitors to the NHLBI PWS system, including website traffic, traffic sources, bounce rate, time spent on the site, page visits, top viewed pages, and click-through rate.

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

The National Heart, Lung, and Blood Institute (NHLBI) Public Website System (PWS) is the main communication tool used to provide health education to the public related to heart, lung and blood research and news. NHLBI uses the site to inform the public about its mission, vision, organization, events, and programs. In addition, the website is used for community and social services; public services; and to meet the open government requirement. There are two main parts of the NHLBI PWS: the public-facing site that presents NHLBI mission and other education materials to the general public, and the internal-facing site that allows for maintenance of content, as well as access to tools and services.

The public-facing website includes the following distinct interfaces: NIH Centers for Accelerated Innovations - Research Evaluation and Commercialization Hubs (NCAI-Reach) microsite, Aim for a Healthy Weight Body Mass Index (BMI) Calculator, Community Health Workers, We Can!, Chronic Obstructive Pulmonary Disease (COPD) National Action Plan (CNAP) Community Action Tool, Trans-Omics for Precision Medicine (TOPMed) Program Website, Genome-Wide Repository of Associations Between Single Nucleotide Polymorphisms (SNP) and Phenotypes (GRASP) search tool, Developmental Biology, and Healthy Eating microsite.

The internal-facing website includes the following interfaces: Division of Intramural Research (DIR) Web Services, NHLBI Digital Asset Management (DAM) system and Data Analytics Metric Dashboard.

External links to Archive-It.org and GovDelivery.com may collect PII, which is handled by the third parties. NHLBI is working on a TPWA for those two systems.

The NHLBI PWS maintains and shares information about NHLBI Executive and Division Leadership team, including name, photo, email, staff biography, and position title. The NHLBI PWS maintains and shares information about NHLBI Divisions, including email, phone number, and address.

Contact page maintains mailing address and includes a link to the NIH Enterprise Directory (NED) that maintains its own unique Privacy Impact Assessment (PIA) with all legal authorities documented.

Visitors non-sensitive data regarding portal visit is also collected, which includes: computer Internet Protocol (IP) address, domain, website's Internet address, product and version of the visitor's operating system and browser, date and time the visitor arrived and how long the visitor spent visiting the site (which links/features/pages they clicked/accessed).

The following interfaces collect PII to create an account, and provide a link to access those accounts by 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.

NCAI-Reach microsite collects email, username, password and organization for account creation.

CNAP Community Action Tool microsite collects email, username, password and organization.

Developmental Biology microsite collects name, email and phone number.

Healthy Eating microsite collects email and password.

Aim for a Healthy Weight microsite's BMI Calculator page collects height and weight.

We Can! microsite collects email and comments.

GRASP search tool microsite collects visitor's name, email, study title, publication date, study subject's ancestry

TOPMed Program Website collects name, email, professional title, phone number, fax number, degree, organization, department, address, city, state, zip code, country, study title, publicati

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
Device Identifiers
NED ID
Username and password
Organization name, department name, degree, study title, publication name, publication date, study subject's ancestry
height, weight, comments, fax number, laboratory name, pdf documents, visitor web metrics
Media assets such as images, video, voice recordings

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

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

Creation of accounts to receive alerts and informational updates.

Device Identifier information is used in web usage data analytics.

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

None

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

42 USC § 285b

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OMB 09-25

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

OMB 0925-0648: Generic Clearance for the Collection of Qualitative Feedback on Agency Service Delivery (NIH) Expiration Date: July 31, 2027

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 NHLBI Privacy Policy is available from a link directly on the NHLBI Public Website footer banner. It includes the details that will be collected while they visit the NHLBI Public Website.

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 NHLBI public website has the following opt-out options:

Cookies: The Privacy Policy page provides instructions “How to Opt Out or Disable Cookies”. If you opt out of cookies, you will still have access to all information and resources at NIH.gov.

Surveys: Occasionally, we use pop-up forms to obtain feedback from visitors on how well the site is meeting their needs. Any time this happens, you are free to close the window and resume browsing; you are not required to provide any information in order to use this site.

Emails: if you send us an E-mail, and you are worried because your communication is very sensitive, you can send it by postal mail instead.

Online Forms: Certain areas like the "NHLBI Online Catalog" and the "Join the Health Information Network" include forms where you actively enter your personal information. You do not have to

provide this additional information to receive the service.

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

Individuals with active accounts whose PII is in the system are notified by an email. If their accounts are no longer active, they are not notified.

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 concerned about inappropriately obtained, used, disclosed or is inaccurate will be directed to contact the Institute's Privacy Coordinator.

There is a link on the NHLBI Privacy Statement and Comment Policy page allows a site visitor to email the NHLBI Privacy Act Officer directly.

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) at the source level by relevant NHLBI program/project staff, information security team, and/or privacy coordinators to ensure the account's PII data's integrity, availability, accuracy, and relevancy. Stale accounts (and associated PII) is removed from the system as needed.

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.

All requests for administrative rights, regardless of privileged user role, must be approved. Active Directory (AD) groups are used to assign and control administrative rights to the domain or to an individual computer. Application administrative access is granted via either the application itself, or User Manager (for legacy applications).

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.

The principle of least privilege and need to know is used, allowing only authorized accesses for users which are necessary to perform primary job responsibilities in accordance with organizational missions and business functions.

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. Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials. Administrators and Privileged Users require additional training specific to their roles and responsibilities.

Describe training system users receive (above and beyond general security and privacy awareness training).

Administrators and developers are trained on the features and functionalities of applicable systems/applications. The frequency of this training will be initially at the start of project on-boarding, one-on-one in person training as well as online training on an as-needed basis.

Users requesting remote access are required to take specialized training courses to include Securing Remote Computers and complete a Remote Access User Certification Agreement.

Users requesting Administrative rights to their assigned computers are required to complete Systems Administrator Training.

There are also role-based training requirements for staff designated as having "Significant IT Security Responsibilities." These include HHS role-based training courses for Executives, Managers, and IT Administrators.

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 Authority Agency (DAA): 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

Item 10-102-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. This includes:
• documents such as letters, memoranda, reports, handbooks, directives, manuals, briefings, or presentations created on office applications, including those in Portable Document Format (PDF) or its equivalent
• senders' and recipients' versions of electronic mail messages that meet the definition of Federal records, and any related attachments
• electronic spreadsheets
• digital still pictures or posters
• digital video or audio files
• digital maps or architectural drawings
• copies of the above electronic records maintained on websites or web servers, but EXCLUDING

web pages themselves
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 - Management oversight of activities, security awareness and training for users of the system, conduct disaster recovery exercises, separation of duties for personnel administering the system, isolating development test instances of the system.

Technical controls - Secure Socket Layer (SSL) for browser to server communication. User authentication (login) and logical access controls, anti-virus software, fire walls, role based access through application. The database is behind a fire wall, with no direct access to it from outside the network. Password complexity requirements for all user accounts. Password clipping levels established to lock accounts that use incorrect password more than 5 times.

Physical controls - Server housed in secure facility, climate control, fire alarm, fire extinguishers and Uninterrupted Power Supply (UPS) for servers.

Identify the publicly-available URL:

https://www.nhlbi.nih.gov
https://healthyeating.nhlbi.nih.gov
https://developmentalbiology.nih.gov/index.php
https://topmed.nhlbi.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.

Other technologies that do not collect PII:

Adobe Analytics

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