US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/14/2016

OPDIV:

OS

Name:

Office of Disease Prevention and Health Promotion Web Sites System

PIA Unique Identifier:

P-2362958-028744

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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.

The Healthypeople site was converted to Drupal Content Management System (CMS).

As of November 2015 the Visiting Scholar application is no longer handled by an Office of Disease Prevention and Health Promotion (ODPHP) website.

Describe the purpose of the system.

ODPHP Web Sites System is a collection of web sites (including healthfinder.gov) that provide guidance on health matters to the public via the Internet.

The National Health Information Center (NHIC) mandate is to provide a single point of access to the full range of health information for consumers and professionals that is available from public agencies; professional, nonprofit, and educational organizations, and other appropriate resources.

OS Office of the Assistant Secretary for Health (ASH) ODPHP Web Sites is a collection of web sites. The ODPHP Web Sites System includes the following web sites (healthfinder.gov, healthypeople.gov, and health.gov) as described below:

Healthfinder.gov provides plain language information to help consumers make informed decisions about their health. It's been providing health information resources from the federal Government and its many partners since 1997.

Healthy People – Healthy People provides science-based, 10-year national objectives for improving the health of all Americans.

Health.gov provides information about many of ODPHP's initiatives, including the Dietary Guidelines for Americans and the Physical Activity Guidelines for Americans.

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

The information on ODPHP Web sites includes as much information as possible on prevention and wellness health issues from many sources, both public and private.
Limited PII includes the names, e-mail, phone number, mailing address.

User credentials for the public consist of a email address and password. Users can opt out of providing this information but will not receive email updates.

System Administrator HHS user credentials are stored on the ODPHP Website.

HealthyPeople.gov has been converted to use the Drupal CMS which now adds the ability for users to login using their user name and password.

Users that elect to use the healthfinder.gov content syndication platform are asked for the following information: email address, password, organization's name, first and last name. This information is only used to follow up with users if a major change required users to take action.

ODPHP hosts an informative blog covering current health related topics. Participants email information is collected to include these individuals on future blog posts and topical listservs.

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

Congress has mandated the creation of the National Health Information Center (NHIC), which is operated by the ODPHP. The NHIC mandate is to provide a single point of access to the a broad range of health information, particularly on prevention and wellness, to be made available to consumers and professionals. Sources of this information include public agencies; professional, nonprofit, and educational organizations; and other appropriate resources. This information is collected and consolidated on Web sites under ODPHP's oversight.

ODPHP oversees Web sites that meet the NHIC's goals in four broad areas:

Information management: ODPHP collects and manages information on the prevention of disease and negative health outcomes. It develops and manages content including databases and Web sites, and produces both original content as well as content from other sources, edited to be more broadly understandable to the public.

Web site management. ODPHP maintains the functionality, security and availability of several Web sites, including portals and sites that support ODPHP activities and HHS initiatives. Website managers are requires to have a current HHS IT Account and Administrative Account Access. Administrators gain access to the website is through an individual unique login and password which is issued to them by ITIO.

Collaborative workspace. ODPHP provides Web 2.0 and social networking features and tools for health professionals and intermediaries, permitting them to exchange ideas and to further ODPHP's mission.

The public can contact NHIC via email to get connected with organizations that provide reliable health information.

Other information included: Names, Address, Street, City, Zip, Country, email.

This information is not stored on the Health.gov website or ODPHP server but is passed through email to a NHIC Mailbox for review and response. All submissions of PII are voluntary. Email address and phone number information is collected in order to respond to requests for information.

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

Registering users may submit the name of their organization and job title Other information included:

HHS User Credentials

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Any person can register for a login to HealthyPeople.gov or for the content syndication component of HealthFinder.gov.

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

ODPHP Web sites include resources such as public blogs, and allow individuals to volunteer to make informational posts. Contributors must first apply, and are granted access if they are able to supply a valid e-mail account. They may then choose to make postings, which will include their names and organizations along with the information or ideas posted.

Emails for blogs are used and to contact with updates for informational purposes only.

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

PII will not be used for any secondary purposes

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

The ODPHP was established by the National Consumer Health Information and Health Promotion Act of 1976 (Section 1706 of the PHS Act as amended) and continued under the "Omnibus Health Act of 1988," was mandated a number of responsibilities, including participation in policy development; oversight and coordination of HHS activities in disease prevention and health promotion; identification of unmet needs related to health information and disease prevention and development of resources to meet such needs; and dissemination of health information.

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.

Persnl. Rcrds. in Operating Offices 09-90-0018

Identify the sources of PII in the system.

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Media/Internet

Private Sector

Identify the OMB information collection approval number and expiration date

An information collection approval is not required because only contact information is requested to enable the system to provide a login to the subscriber to HealthyPeople.gov or for the content syndication component of HealthFinder.gov. Applicant information is properly discarded after it is reviewed.

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.

There is no process to notify individuals that their PII will be collected. Individuals are aware of what PII is being collected because the data subjects submit their PII directly. The main purpose for collecting the PII is only to allow access to the system. There is a separate process that is handled outside of the website through email communication with ODPHP. The application form users are notified that their information will be emailed and that they will receive a follow up email from ODPHP if they are selected.

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.

Individuals are aware of what PII is being collected because, in all instances where PII is collected, the data subjects submit their PII themselves and is not shared or used for any purpose other than the purpose for which the information is submitted.

Individuals who submit PII, submit their PII with the intent of having it be used in this way. In the course of using the system, individuals are supplied with privacy, security, and Freedom of Information Act (FOIA) disclaimers.

User credentials are only stored to allow users repeated access to the web site. Users can opt out of submitting their information by not signing up for login access. The access is not required to access any publicly facing portion of the site and is only necessary to submit stories to be displayed on the site.

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

The data subjects submit their PII themselves and is not shared or used for any purpose other than the purpose for which the information is submitted. No major changes to the system that would affect the way in which the information is used are anticipated.

Individuals provide their contact information because they wish to use the system to learn and share information. That is the only reason for which the information is collected.

If a major change were to happen to the way that user's personal information is used then those users would be notified ahead of time through email to confirm their willingness to display their information.

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 users believe their information has been misused in any way, contact information for the system owner is provided. Additionally, the FOIA Appeals Process point of contact's information is provided in the footer of every Web site.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Information is submitted by the data subjects themselves, and is; therefore, assumed to be accurate. Any suggestion made by a member of the public that information were inaccurate would be investigated and altered appropriately.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Create blog entries and other informational posts

Administrators:

Perform administration of servers

Developers:

Provide support for databases and Web servers (e.g., provide Internet Information Services (IIS) and .NET support)

Contractors:

Administration of servers and software maintenance. These are direct contractors with proper HHS credentials

Others:

An ODPHP Public Health Advisor who is responsible for reviewing/approving visiting scholar applications

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Public comments and blog posts are reviewed and moderated by agency staff prior to publication. Physical Activity Guidelines for Americans (PAG) Supporter Network:

Form submissions are stored in a moderation queue in a secure Structured Query Language (SQL) Server database. Administrators review submissions regularly and approve new entries for public display on the website as appropriate. The only information shown on the website is the organization's name and state. User information is never displayed to the public — it is only stored in case ODPHP needs to follow up with the individual about usage or changes to the application.

Information is stored until a user requests removal from the system. When a user is removed, their information is permanently deleted from the database.

Confirmation emails are automatically generated and delivered to the email submitted (Confirmation emails only contain a link to access their new Application Programming Interface (API) key — this can't be used to access the system without additional information.)

In addition, there are processes in place specific to the Healthy People Consortium:

Users must be logged in to Drupal prior to accessing the submission form. When logged-in users enter information, it is stored in Drupal's MySQL database. Only users with the role of Consortium User or top-level Admin have access to this information.

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 website administrators have access to PII such as email contact information to follow up with individuals related to the content or posting of their blog posts.

Specific admin roles are setup in Drupal to ensure that only the appropriate administrators have access to information. For example: the administrator role for stories from the field stories only has access to Stories from the Field related user submissions.

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.

ODPHP complies with the security training requirements set by the HHS Office of Information Security. System users are required to take annual on-line training for Privacy Awareness, general Information Systems Security Awareness.

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

In addition, ITIO provides the following Role Based Information Training for Executives, IT Administrators and Managers:

Information Security for Executives
Information Security for IT Administrators
Information Security for Managers

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.

General Records Schedule (GRS) 3.2. Item 010, Disposition Authority: DAA-GRS-2013-0006-0001. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

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

The server host location, employs multiple levels of perimeter protection to prevent unauthorized access and information disclosure. All PII collected resides on servers in a government secured facility. The system undergoes an annual Certification and Accreditation review, as well as Security Testing & Evaluation of all sites and servers every 3 years. All remote server access is restricted on as needed basis and is password protected. Access to the building that houses the Data Center is restricted to authorized employees, and access to the Data Center itself is restricted further. Only government credentialed personnel with specific access to the Data Center may enter the facility, all access is logged and monitored. Access to the servers that store PII are restricted to HHS authorized VPN users, who have been granted access to the ODPHP environment. All servers and Web sites are monitored for unauthorized access attempts, there are procedures in place to address any such findings. Additionally, only ODPHP administrators are allowed to connect and interact with the servers. Administrator accounts are strictly monitored and reside on an Active Directory controller specific to the ODPHP environment. All personnel who have access are required to pass HHS privacy training.

Identify the publicly-available URL:

www.healthfinder.gov

www.healthypeople.gov

www.health.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?

No

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.

Session Cookies that do not collect PII.

Does the website have any information or pages directed at children under 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?

No