US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/21/2016

OPDIV:

OS

Name:

Office of Women's Health Websites

PIA Unique Identifier:

P-3557958-400588

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?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Describe the purpose of the system.

The purpose of the Office of Women's Health (OWH) Websites is to provide woman-specific health information and resources to women, girls, and health care providers. This information is disseminated through the OWH Websites (womenshealth.gov and girlshealth.gov) and also through their email service, GovDelivery.

Health information and resources on the Websites include information about issues that are specific to women and girls. For example, the Websites include extensive information about menstruation, pregnancy, birth control, and related health issues, such as breastfeeding and post-partum depression. The Websites also address topics such as polycystic ovary syndrome (PCOS), sexually transmitted infections, the role of nutrition and fitness in the health of women and girls, important annual screenings for women (such as Pap tests and mammograms).

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

The system will be used to maintain and disseminate public health information. Examples of public health information include:

Announcements about upcoming health observances, such as National Women's Health Week and National Women and Girls HIV/AIDS Awareness Day.

Blog posts highlighting women's health topics, such as breastfeeding tips and resources, what you can do to protect yourself against Zika, HHS resources for pregnant women and new moms, importance of getting regular cancer screenings, and HHS resources for caregivers.

The Office on Women's Health (OWH) Website, womenshealth.gov, provides a form that enable users to subscribe to OWH's email lists, on GovDelivery. The GovDelivery form collects only user email addresses (stored in the GovDelivery application) for the purpose of pushing period notifications about womenshealth.gov topic pages that have been updated. The same form that submits user subscription information to GovDelivery is embedded in the womenshealth.gov application. GovDelivery is a unidirectional platform, in that email notifications are only pushed out to subscribers, and it does not serve as a way for subscribers to provide input to or correspond with OWH.

The womenshealth.gov Website also has a contact form here: womenshealth.gov/contact-us/email/. This form submits any information the user inputs into womenshealth@hhs.gov. The contact us form does not capture or store any of the form data and only emails the user's information to OWH.

Drupal the web content management system (application) also stores login credentials for privileged users (federal employees and direct contractors). Privileged user credentials consist of user email address, password, and Internet Protocol (IP) address. The web content management system has its own Privacy Impact Assessment (PIA).

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

The Office on Women's Health (OWH) Websites will be managed using Drupal. Drupal is an HHS-approved web content management system.

All health content and resources will be maintained, updated, and archived in accordance with OWH's annual editorial calendar. The health content maintained throughout the OWH Websites is expert reviewed and cleared through the HHS Assistant Secretary for Public Affairs (ASPA) before being posted on the public sites. All other content pertains to OWH initiatives and health observances, and is reviewed by OWH senior leadership before being promoted to production.

GovDelivery collects and stores subscriber email addresses. Those addresses are stored until one of the following happens:

Subscriber unsubscribes from the GovDelivery list.

Email sent to a subscriber bounced back (is undeliverable), in which case that email address is purged automatically from OWH's lists.

Credentials for system administrators are also stored in GovDelivery. System administrator credentials include an email address and a password. Only federal employees and direct contractors are system administrators.

Privileged users (federal employees and direct contractors) of the web content management system (application) login via multifactor authentication. In addition to storing their user credentials, the application also tracks and records their actions within the application.

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

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

Employees

Public Citizens

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

GovDelivery: Email addresses may be provided by members of the public via a GovDelivery embedded web form. GovDelivery is an opt-in email distribution service that enables people to subscribe to receive updates about specific health topics or health observances. The Office on Women's Health (and many other Department of Health and Human Services agencies) uses GovDelivery to email news to people who have subscribed to receive updates.

Web Content Management System: The application uses multifactor authentication to verify privileged user identity. This includes the user's email address, password, and an approved IP address.

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

The email address will not be used for secondary purposes.

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

The Office on Women's Health was created under the Department of Health and Human Services Office of the Secretary, Office of the Assistant Secretary for Health, in 1991. It is also established in section 229 of the Affordable Care Act.

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.

Not Applicable

SORN is In Progress

Identify the sources of PII in the system.

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

N/A

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 form tells users that they are submitting their email address to subscribe to receive more information about a specific health topic or Office on Women's Health observance.

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.

When users first subscribe, they are provided with opt-out instructions. Also, all email messages sent from GovDelivery have a prominently displayed "Unsubscribe" link, as well as the Office on Women's Health (OWH) toll-free help number and a link to OWH's email address, in case they have trouble unsubscribing.

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

If a major change were to occur, the Office on Women's Health would notify users and obtain their consent before using their email addresses in some other way.

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.

All messages to individuals include several ways for people to get in touch with the Office of Women's Health (OWH). People may email or call OWH's help desk (toll-free number), or unsubscribe. The unsubscribe function is automated, through GovDelivery, and OWH's email address and help desk are monitored by full-time, dedicated staff.

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

GovDelivery: All email addresses that no longer work are automatically purged from the system. In addition, users who opt out (unsubscribe) are automatically purged from the system. This ensures that only relevant subscriber data are included and ensures that the system only distributes email to accurate and available email addresses. It also maintains the integrity of the system by ensuring that people who have opted out do not receive unwanted emails.

Web Content Management System (application): The application inherits HHS rules for password complexity, longevity, and login attempts, thus ensuring credential integrity. All accounts are granted and removed under the sole authority of the system owner, ensuring that all active accounts are both accurate and relevant.

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

Administrators:

Create/remove accounts, assign access privileges; e-blast content creation and HTML template construction

Contractors:

Direct contractors update and publish content in the Web Content Management System and development themes and templates.

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

Access to The Office on Women's Health (OWH) GovDelivery account is limited to federal employees who are responsible for the creation, review and distribution of OWH news announcements, and for the management of website content.

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.

GovDelivery: is set up only to collect email addresses and only to distribute email messages to topic subscription lists.

Web Content Management System (application): The application supports multiple user role and granular permissions, based on role. The system owner controls how and to whom roles are assigned. Thus, people who only need to edit and create content cannot make other changes within the application; nor can they view information about other users. Only the application owner and system administrator can access all of the data in the application.

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.

All personnel who access Office on Women's Health IT systems complete annual HHS security awareness and privacy awareness training courses.

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

Administration tutorials and in-person, one-on-one training with an experienced administrator are provided.

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.

GovDelivery: Email addresses are automatically removed when GovDelivery receives bounced email from those addresses. We have reviewed the Department of Health and Human Services email records retention policy (National Archives and Records Administration's (NARA) Bulletin 2013-02: Guidance on a New Approach to Managing Email Records). The public announcements included in our GovDelivery announcements are exempt from the kinds of email communications we are required to retain. However, we do have a record of every bulletin we have sent from GovDelivery. All communications via GovDelivery are outgoing and not an incoming avenue for queries, which are all received directly via our Office of Communications email address.

User Credentials retention schedule: 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.

GovDelivery: All subscription and login data are transmitted to the GovDelivery system over secure sockets layer (SSL). Administrators are limited to OWH employees. All system administrator credentials are also submitted via SSL. The administrative web portal is secured using SSL and user credentials. The data is not encrypted in the GovDelivery database, but the database is only accessible directly from within GovDelivery’s network, and only select individuals have access to the database. Not all GovDelivery employees can access it and they have strict polices as to who may do so. GovDelivery's security policies are regularly audited and tested to ensure that the data is secure and cannot be breeched.

Web Content Management System (application): All privileged users login via SSL and using multifactor authentication, and credentials are hashed before being transmitted to the database. The database itself is encrypted and resides behind a firewall and can only be accessed by the application itself or by qualified, credentialed IT staff.

Identify the publicly-available URL:

womenshealth.gov, girlshealth.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.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Other technologies that do not collect PII:

Google Analytics and CrazyEgg

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

Yes

Is there a unique privacy policy for the website, and does the privacy policy address the process for obtaining parental consent if any information is collected?

Yes

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