

US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

January 30, 2025

OPDIV:

OS

Name:

Office on Women's Health GovDelivery

TPWA Unique Identifier:

T-6341928-777132

Is this a new TPWA?

Yes

Will the use of a third-party Website or application create a new or modify an existing HHS/OPDIV System of Records Notice (SORN) under the Privacy Act?

No

If SORN is not yet published, identify plans to put one in place.

null

Will the use of a third-party Website or application create an information collection subject to OMB clearance under the Paperwork Reduction Act (PRA)?

No

Indicate the OMB approval number expiration date (or describe the plans to obtain OMB clearance).

Expiration Date: 1/1/01 12:00 AM

Describe the plans to obtain OMB clearance.

Explanation: null

Does the third-party Website or application contain Federal Records?

No

Describe the specific purpose for the OPDIV use of the third-party Website or application:

OWH offers a variety of digital bulletins for specific categories (i.e. under Womenshealth.gov (health topics and social media), under Girlshealth.gov (news, parents and caregivers, teachers and educators, social media, and health topics). These topics can be subscribed to by the public and can be delivered as e-mails through the govDelivery platform.

Have the third-party privacy policies been reviewed to evaluate any risks and to determine whether the Website or application is appropriate for OPDIV use?

Yes

Describe alternative means by which the public can obtain comparable information or services if they choose not to use the third-party Website or application:

None

Does the third-party Website or application have appropriate branding to distinguish the OPDIV activities from those of nongovernmental actors?

Yes

How does the public navigate to the third party Website or application from the OPDIV?

Other...

Please describe how the public navigate to the thirdparty website or application:

OWH provides an email entry form embedded at the bottom of their homepage. Once the subscriber enters their email address, they are brought to <https://public.govdelivery.com/accounts/USOPHSOWH/subscriber/topics>. This is referred to as a Signup Builder page in govDelivery and is hosted by govDelivery. Once the subscriber fills out all required information and a CAPTCHA, they are given the topic menu as seen in the first image.

If the public navigate to the third-party website or application via an external hyperlink, is there an alert to notify the public that they are being directed to a nongovernmental Website?

Yes

Has the OPDIV Privacy Policy been updated to describe the use of a third-party Website or application?

Yes

Provide a hyperlink to the OPDIV Privacy Policy:

<https://www.hhs.gov/privacy.html>

Is an OPDIV Privacy Notice posted on the third-part website or application?

Yes

Is PII collected by the OPDIV from the third-party Website or application?

Yes

Will the third-party Website or application make PII available to the OPDIV?

Yes

Describe the PII that will be collected by the OPDIV from the third-party Website or application and/or the PII which the public could make available to the OPDIV through the use of the third-party Website or application and the intended or expected use of the PII:

Email address. Used only for communication purposes through govDelivery.

Describe the type of PII from the third-party Website or application that will be shared, with whom the PII will be shared, and the purpose of the information sharing:

Email address which is used only for communication purposes through govDelivery. The email addresses are not shared with anyone. Administrators in the HHS govDelivery Account, as well as Granicus Account Management Staff, have access to the data in the govDelivery platform. Granicus Account Management staff can access the email addresses when needed to aid govDelivery customers with requests and support issues.

If PII is shared, how are the risks of sharing PII mitigated?

Email address. Used only for communication purposes through govDelivery. No sharing of

Will the PII from the third-party website or application be maintained by the OPDIV?

No

Describe how PII that is used or maintained will be secured:

All data secured at rest and in transit through Federal Information Processing Standard (FIPS) 140-2 validated encryption. Data in transit utilizes Transport Layer Security (TLS) 1.2. Data at rest is

encrypted at the hardware and database level with AES256 encryption algorithm. All encryption keys are stored in a separate vault called a hardware security module or an HSM.

What other privacy risks exist and how will they be mitigated?

Administrator access is the only way to access any PII data. Access is protected through email/password-based authentication and TLS 1.2 encryption.