US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

September 20, 2017

OPDIV:

OS

Name:

OS/GitHub/HHS source code

TPWA Unique Identifier:

T-7193023-764832

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.

N/A

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: N/A

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:

The specific use of the service uses the capability to define teams and associate both user accounts and repositories with the teams to create an HHS organization area within GitHub for consolidating multiple source code repositories and centralizing their access management. The Health and Human Services (HHS) organization area contains both public repositories, visible to anyone accessing the GitHub site, and private repositories that only members of associated teams can see. Changes can be proposed by anyone that can see a repository, but must be approved by a member of a team specifically granted permission to incorporate changes.

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:

Members of the public can obtain descriptions and contact information from the Health and Human Services (HHS) Source Code Inventory, published on the agency's primary website at https://www.hhs.gov/code.json.

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 OPIDIV?

An external hyperlink from an HHS Website or Website operated on behalf of HHS

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

The HHS Source Code Inventory is published on the agency's primary website, in compliance with the Federal Source Code Policy, as a downloadable file rather than as part of a web page. Some of the entries in the inventory file contain hyperlinks to source code repositories on GitHub. Since the inventory file is not directly displayed in web browsers, public visitors to the agency website cannot browse the inventory and select a hyperlink to be redirected to GitHub. Instead, visitors must save a local copy of the inventory file and use other software, such as a text editor, to display the contents. The hyperlinks to GitHub can then be copied from the local copy of the inventory file into a web browser address bar. Since the hyperlinks to GitHub are not embedded on any agency website page, there is no corresponding alert.

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 anongovernmental Website?

No

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:

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?

No

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:

Each repository on GitHub has an associated issues log that enables free-form messages to be entered by anyone with a GitHub account that can see the repository. Members of the public may voluntarily provide PII in the body of their issue log entries, even though they are not required or encouraged to do so. Additionally, when GitHub account holders perform actions on the repositories, such as submitting a request for code changes or entering an issues log entry, GitHub associates the action with the account. Members of the public may choose to provide their real names, photographs or e-mail addresses in their account profiles, which then become available by association with any action they take on an HHS repository. HHS does not use the PII made available from the TPWA and has no intended or expected use of the data.

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:

There is no PII that will be shared.

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

Not Applicable

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:

Not Applicable

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

Messages recorded in a repository's issues log could potentially include PII, voluntarily provided by the person entering the message, since the messages are free-form text. HHS organization account administrators are notified when new issue log entries are made and will moderate them to mitigate the exposure of PII. Additionally, GitHub users can associate their names, e-mail addresses and photographs with their accounts, which can then be associated with repositories they "watch" or "star". The GitHub users can mitigate those privacy risks themselves through personal privacy settings.