US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

January 25, 2018

OPDIV:

OS

Name:

Agari – Enterprise Protect

TPWA Unique Identifier:

T-8930556-926434

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:

The Agari service is utilized by HHS to monitor and improve its deployment of Domain-based Message Authentication, Reporting & Conformance (DMARC) as directed by DHS Binding Operational Directive 18-01.

The service allows HHS to continually monitor and improve the security and delivery of our mail-based outreach. It protects the public trust in HHS by stopping phishing attacks against HHS constituents and identifying malicious domains for lawful seizure or take down.

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:

Site and associated data are not available to the public.

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

No

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

Site and associated data are not available to the public.

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

N/A. The Agari web service application is restricted through authentication to HHS staff, who access the site with any standard browser.
https://cp.agari.com/account/login

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?

No

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?

No

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:

Names and emails of HHS administrators and users are maintained to establish roll-based access controls.

As defined by the DMARC RFC, HHS requests service providers to send samples of mail failing authentication to the Agari service for our analysis. The failure samples only include the relevant mail headers and any URLs within the body of the email because these are relevant for risk assessment and incident response.   No other data is provided.

In some cases, the email failure samples can include personal or work email addresses of an individual in the from: field and the sample will include email subject. This data will only contain PII when mail is forwarded by an individual through a participating service.

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:

Information is accessed and viewed by HHS staff to troubleshoot mail systems, ensure the trusted delivery of outreach mail and assess email-based risk to HHS constitutents.

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

All mail failure samples are maintained for 14 days and then deleted. Thus any PII associated with

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:

Any PII is held for 14 days and then destroyed. Otherwise, the data is viewed online only. All access is via HTTPS.

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

None.