

US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

October 02, 2020

OPDIV:

OS

Name:

Workcast

TPWA Unique Identifier:

T-4548424-448014

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 purpose of Workcast is to collect email addresses, first name, last name and state from the public in order to register for the Office of Minority Health's COVID-19 Virtual Symposium.

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:

The public may go to Minority Health Website (MHW) to view the presentations and recorded video from the Virtual Symposium after the event has concluded.

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?

Incorporated or embedded on HHS Website

Please describe how the public navigate to the third-party website or application:

The public has the option of adding their email address after selecting a link on the MHW that takes them to a Workcast.com page where they can enter their email to register for the event.

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.minorityhealth.hhs.gov/omh/Privacy.aspx>

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:

Participants enter their email addresses into a sign up page on Workcast. Both the user and Office of Minority Health (OMH) administrators have access to Workcast to remove a participants email address if they chose to not register before the event. The user can unsubscribe via a link he/she received in the message from Workcast or an administrator can unsubscribe a user through logging into Workcast.

OMH Administrator will not collect the Personally Identifiable Information (PII). Access to PII only for administrative purposes.

Email addresses, first name , last name and state (user credentials) are stored within Workcast and not on OMH's website.

Participant registration data will be destroy on the Workcast once the symposium is over.

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:

The PII is not shared with anyone. The PII information is only for symposium registration purpose.

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

N/A

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:

Data Retention

Workcast hold records of Client Data and processing activities and confirms that security and organizational measures are in place in order to ensure that its obligations under (General Data Protection Regulation) GDPR are complied with.

All clients of Workcast have the right to access, delete and transfer any data which Workcast holds about them (including their Personal Data), relating to the contract and services delivered in relation to said contract. If the Client wishes to make such a request, it should be submitted to support@workcast.com and Workcast shall respond within 5 days of receipt.

Under the GDPR, Workcast requires consent in order to retain any Personal Data which relates to the Client (unless it can rely upon another ground of lawful processing) and the Client has the right to opt out of such data retention.

Data Security

To protect data stored on our servers, we regularly audit our system for possible vulnerabilities and attacks, and we use only secured access tier 1 data centers. Workcast maintain International Organization for Standardization (ISO):270001 information security controls.

Workcast shall comply at all times with the Information Commissioner's Office (ICO's) code of practice on Privacy Impact Assessments and has a designated individual to take responsibility for data protection compliance.

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

No other privacy risks exist that we are aware.