Privacy Impact Assessment (PIA): CDC - OHE Qualtrics - QTR4 - 2023 - CDC7034059

Created Date: 11/9/2023 3:01 PM Last Updated: 3/14/2024 12:01 AM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	CDC - OHE Qualtrics - QTR4 - 2023 - CDC7034059	**PIA ID:**	1734020
Name of Component:	CDC - OHE Qualtrics System	**Name of ATO Boundary:**	OHE Qualtrics System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	154
Submission Status:	Re-Submitted	**Submit Date:**	2/5/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC7034059
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Initiation
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	2/26/2024
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	The OHE Qualtrics platform is a third-party web-based application that allows Government agencies to create surveys and then collect, analyze, and store the data produced from those surveys. Government agencies can use the application to collect and analyze citizen, employee, and community feedback to improve services and engagement for both external customers (citizens) and internal customers (public sector employees). The OHE Qualtrics platform enables multiple departments within an agency to collect and analyze survey data within a single enterprise system, allowing all levels of the agency or department to have access to important feedback data. The OHE Qualtrics platform includes an array of services that can be utilized to track, manage, and improve the experience of external and internal customers.

PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	OHE Qualtrics platform collects customer satisfaction surveys only. First name, last name, phone number, sexual orientation and ethnic/religious affiliation information is collected but not correlated. Some emails are stored on a voluntary basis.
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	Non-HHS User Credentials Username Password
PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	First name, last name, and email addresses are collected for the purposes of administering surveys to CDC personnel and interns only. Sexual orientation, ethnic and religious data are collected for health equity purposes and to develop evidence based strategies. No data is shared with another system outside OHE Qualtrics.
PTA - 7:	Does the system collect, maintain, use or share PII?	
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	Purpose of the website is for Admins and Staff to create and disseminate surveys to CDC personnel. Survey takers receive a link where they are prompted to enter first name, last name, and email to complete surveys. Survey takers do not authenticate for login, data is entered only for the purposes of completing the survey, There are two administrative personnel and eight staff personnel.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Web bug/beacons - Does Not Collect PII Session Cookies - Does Not Collect PII Persistent Cookies - Does Not Collect PII Other technology - Does Not Collect PII
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No

PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Other - Free text Field - Sexual orientation, Ethnic origin
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	501 - 2000
PIA - 4:	For what primary purpose is the PII used?	Creation and dissemination of surveys to collect, analyze, and store such data produced from those surveys. Agency uses the application to collect and analyze citizen, employee, and community feedback to improve services and engagement.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	None.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	S.4486 - Health Equity and Accountability Act of 2022, Public Health Service Act (42 U.S.C. §247d. Public health emergencies).

PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Name, email address
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	No valid SORN record for consistent with collection. Not Applicable.
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Email
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	Surveys are only collected for CDC employees and contractors. OMB Control Numbers do not apply to data collections from agencies, instrumentalities, or employees of the United States in their official capacities. Use of Qualtrics application website does not create an information collection subject to OMB clearance.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	Participation in all surveys is optional. Surveys can be opted out of completely from the Qualtrics link. If they do opt out, they break agreement to be in the program.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	Survey participants PII information is stored exclusively in the cloud Qualtrics systems and is not extracted in meaningful form. If the Qualtrics system or other PII data is disclosed, or changed individuals are sent a notification email.
PIA - 15:	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. If no process exists, explain why not.	Surveyor administrators will contact survey staff and notify them of unlawful disclosures, use or inaccuracies.

PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	Survey data is pulled primarily from business contact information available from CDC employee data. Verification takes place when survey participants submit data.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators
PIA - 17A:	Select the type of contractor.	
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	System administrators manage survey administrators (users) in the Qualtrics environment, and survey administrators to administer customer satisfaction surveys. Survey takers do not exist in the system as users.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	CDC employees are the only users accessing the system, CDC performs administrative safeguards during onboarding. Qualtrics system and data, including the PII contained in the system is secured according to FedRAMP and CDC security guidelines. The CDC SSP Security Plan covers this system. These controls include the enforcement of user roles and by having users agree to system Rules of Behavior and taking mandatory CDC Security Awareness Training and Records Management training at least annually. Privileged access to Qualtrics is granted solely by Qualtrics program management, adhering to the principles of role-based access and least privilege
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	Technical: Qualtrics system is a FedRAMP approved cloud system that adheres to a risk-based approach for the adoption and use of cloud services by the federal government. Qualtrics administrators create unique role-based profiles for each user and assign users to groups and determine controls and background clearance levels associated with each user and group. Login is granted by a centralised OHE administrator through username/password and is currently in the process of being utilising Personal Identity Verification card access through Active Directory.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (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.	Annual Security Awareness and Privacy Awareness training provided by CDC is. Surveyors position specific to the CDC employees title.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	CDC Ethics Training.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	Records are disposed of in accordance with CDC ATSDR: 1-19 Management Surveys (studies), (NC1-90-78-1, Item 19) and NARA General Records Schedule 40 Office of Government Ethics program questionnaire records.

PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative: CDC employees are the only users accessing the system, CDC performs administrative safeguards during onboarding. Qualtrics system and data, including the PII contained in the system is secured according to FedRAMP and CDC security guidelines. The CDC SSP Security Plan covers this system. These controls include the enforcement of user roles and by having users agree to system Rules of Behavior and taking mandatory CDC Security Awareness Training and Records Management training at least annually. Privileged access to Qualtrics is granted solely by Qualtrics program management, adhering to the principles of role-based access and least privilege Technical: Qualtrics system is a FedRAMP approved cloud system that adheres to a risk-based approach for the adoption and use of cloud services by the federal government. Qualtrics administrators create unique role-based profiles for each user and assign users to groups and determine controls and background clearance levels associated with each user and group. Login is granted by a centralised OHE administrator through username/password and is currently in the process of being utilising Personal Identity Verification card access through Active Directory. Physical controls: FedRAMP approved Qualtrics system enforces physical access authorizations to the information system in addition to the physical access controls for the facility in which the system resides.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	2/5/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: February 5, 2024	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	2/6/2024
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	2/15/2024
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski 2/15/2024 - Per CDC email, the OHE Qualtrics is a new system. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	9

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	PTA 7 and 8 didn't sync. Please spell out OHE and ATSDR in next iteration.	**SAOP Review Date:**	3/13/2024
		SAOP Days Open:	27

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Re_ CDC - OHE Qualtrics - QTR4 - 2023 - CDC7034059.pdf	218820	.pdf	2/15/2024 3:39 PM	1

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	11/9/2023	Selected "phone numbers"	
PIA - 7	Data Feed Service, piafrmcdc	11/9/2023	This question must be answered.	
PIA - 8B	Data Feed Service, piafrmcdc	11/9/2023	This answer and your answer in 8 + 8A cannot coexist.	
PIA - 10C	Data Feed Service, piafrmcdc	11/9/2023	This question is about OMB Collection not SORNs	
PIA - 16	Data Feed Service, piafrmcdc	11/9/2023	This answer does not address the question.	
PIA - 18	Data Feed Service, piafrmcdc	11/9/2023	Incomplete. Address Users.	
PIA - 19	Data Feed Service, piafrmcdc	11/9/2023	Please describe the actual administrative safeguards (i.e., policies such as Rules of Behavior, Privacy and Security Awareness Training)	
PIA - 20	Data Feed Service, piafrmcdc	11/9/2023	The system still requires technical safeguards to be in compliance with federal cybersecurity standards. Please describe those actual technical safeguards.	
PIA - 23	Data Feed Service, piafrmcdc	11/9/2023	Incomplete.	
PIA - 24	Data Feed Service, piafrmcdc	11/9/2023	Incomplete.	
PIA - 7	Data Feed Service, piafrmcdc	1/26/2024	^^	
PIA - 18	Data Feed Service, piafrmcdc	1/26/2024	Then why is users selected??	
PIA - 1	LASKOWSKI, JAMES	2/7/2024	The reviewer notes that PTA 7 and 8 did not sync.	
PIA - 20	LASKOWSKI, JAMES	2/7/2024	Please spell out OHE on first usel	
PIA - 23	LASKOWSKI, JAMES	2/7/2024	Please spell out ATSDR on first use.	
PIA - 19	LASKOWSKI, JAMES	2/7/2024	Please spell out FedRAMP and SSP on first use.	

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	3/14/2024 12:01 AM	**History Log:**	View History Log