Privacy Impact Assessment (PIA): CDC - PRISM - QTR3 - 2024 - CDC8380682

Created Date: 7/26/2024 12:01 PM Last Updated: 10/2/2024 12:02 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 - PRISM - QTR3 - 2024 - CDC8380682	**PIA ID:**	2060150
Name of Component:	CDC - Prevention Impacts Simulation Model	**Name of ATO Boundary:**	Prevention Impacts Simulation Model
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	74
Submission Status:	Re-Submitted	**Submit Date:**	9/13/2024
Next Assessment Date:	10/01/2027	**Expiration Date:**	10/1/2027
Office:		**OPDIV:**	CDC
Security Categorization:	Low	**OpDiv PIA ID:**	CDC8380682
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	
5:	Is the system or electronic information collection, agency or contractor operated?	Contractor

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	None
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.	PRISM is an online data simulation modeling tool that allowed scientists and public health officials to input consultative hypothetical case-based scenario. The data inputs representing hypothetical community public health interventions (no PII or confidential information is collected as part of this process). It yields a baseline computation value used to compare the health and economic effects of established and emerging public health intervention in lifestyle policy domains.

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.	PRISM collects: User's information (user's first_last name and email) as part of the registration process to authenticate into using the system. This information is stored in a back-end database managed by Forio Epicenter and later used for login purposes to review past input scenarios or creating a new one. It can be reviewed by system administrators/developers/technical support to provide support. Demographic profile of national average data or input their own (Population Density, % of population > 65 years old, % black or hispanic, % of population living below federal poverty live, Overall death rate ages 30-64; Cardiovascular Disease (CVD) death rate ages 30-64). Intervention categories Activate Smoking Interventions Smoking Cigarette marketing & sales restriction Smoking counter-marketing Workplace smoking bans Smoke-free multi-unit housing Fruit and vegetable promotion Sodium consumption among nonhypertensives, etc.
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 Email Address
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.	Data are collected to support Health policy planners in formulating hypothetical case-based scenario to understand the comparative benefits of different environmental interventions. Information is not shared. User's information (user's first_last name and email) as part of the registration process to authenticate into using the system.
PTA - 7:	Does the system collect, maintain, use or share PII?	
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	Yes
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.	Public health policy planners log into the site to input case-based scenario data. It formulates a baseline computation value used to examine the potential influence of different types of interventions, both established and emerging, for reducing cardiovascular risks.
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?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to 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 User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Members of the public
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?	PII is collected for creating user's login account.

PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	No secondary use
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.	5 USC 301, Departmental regulations
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.	
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.	
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online Non-Government Sources Members of the Public
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.	PRISM is not considered an information collection system. The business contact information is used for system access only and is not subject to the Paperwork Reduction Act or OMB approval.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Private Sector
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Vendor maintains list of user logins.
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)).	There is a contract in place with the vendor to maintain and safeguard the information within the system. There are no agreements in place related to information sharing or disclosure.
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.	Data sharing of business contact information used for logons only occurs with the CDC vendor who operates the website on behalf of CDC. The vendor does not share PII with other organizations.
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.	Users may opt out but will then be unable to access the site. Users will not be able to register for the site without providing a valid email address. Email validation is a requirement for access to the system.

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.	The CDC Business Steward is able to contact individuals via their email addresses if notification is required. There are no changes anticipated to the disclosure or data uses for this system.
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.	Users may email the National Center for Chronic Disease Prevention and Health Promotion (NCCDPHP) mailbox at chronicinformatics@cdc.gov or Project team at info@forio.com.
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.	User credential logins (email addresses) are reviewed annually to ensure the user accounts are still valid.
PIA - 17:	Identify who will have access to the PII in the system.	Developers Contractors
PIA - 17A:	Select the type of contractor.	Third-Party Contractor (Contractors other than HHS Direct Contractors)
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Developers: Troubleshooting and assisting users as requested. Contractors (indirect): Providing user's support.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The Prevention Impacts Simulation Model (PRISM) project leader is responsible for selecting IT personnel (system administrator and developers) ensuring that personnel have controlled access only to what is relevant to their specific work on the project. The contractor will be obtaining the PII (business contact information) which will be used only for system login. No one other than key staff of the indirect contractor will have access to the data. Staff who leave those roles or leave the organization which hosts the site (Forio Simulations) have privileges removed or reduced to appropriate levels.
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.	Projects on the hosting platform have different levels of acesss. "Author" access provides access to source code. "Customer Service" access provides user account access. Staff members are designated with this level of access (only applying to this project) as they are assigned to development or support.
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 IT Security and Privacy for Developers (developers) Bi-Annual Open Web Application Security Project top-ten Awareness Training (every 2 years - software developers) Annual IT Security and Privacy Overview (annual, non-developers)

PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Staff involved in the PRISM application are trained in the administration, development and maintenance of the PRISM software.
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).	The retention and destruction of all data, including PII, follow CDC's Records Control Schedule for Scientific and Research Project Records (N1-442-09-01). PII will be removed before records are archived.
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 controls: Access to PII follows a least privilege model. Administration is handled via special "Author" or "Customer Service" accounts that have the ability to review user list and runs for the purpose of providing support. Additional protections include PII policies; security awareness and training Technical controls: All interaction with the site is over encrypted https connections. User email and name is stored in server-side database, protected by firewall from being accessed directly from outside entities, with encrypted disk volumes; and additional protections include system backup, redundancy measures, intrusion detection, Role-based authorization and authentication with expiration and renewal limits; timeout controls for inactivity; and audit logs. Physical controls: Physical measures, policies, and procedures are in place at the facility to protect information, building, and equipment from unauthorized intrusions, environmental hazard, and natural hazards. Identification and data entry cards are required for physical access.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	9/13/2024
Privacy Analyst Comments:	OpDiv Analyst: Joshua Mosios (Contractor)	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	9/17/2024
		SOP Days Open:	4

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	9/24/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 9/24/2024 Per CDC email (see Supporting Documentation) the ATO is likely blank due to the PRISM system expiring on 5/13/24. And the answer to PTA-7 is "Yes." All comment have need addressed. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	7

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	9/24/2024 Per CDC email (see Supporting Documenta On the next iteration of the PTA, please update the Please provide POC and URL (if applicable). PTA-5A: Please respond "Yes."	**SAOP Review Date:**	10/1/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Re_ CDC - PRISM - QTR3 - 2024 - CDC8380682.pdf	243351	.pdf	9/24/2024 1:41 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 10C	Data Feed Service, piafrmcdc	7/26/2024	This answer does not align with the fact that the system collects business contact information.	
PIA - 16	Data Feed Service, piafrmcdc	7/26/2024	There is no minimal requirement for review.	
PIA - 21	Data Feed Service, piafrmcdc	7/26/2024	Define all acronyms upon first use (OWASP).	
PIA - 11C	Data Feed Service, piafrmcdc	7/26/2024	Remove corporate names and stick to generic identifiers (vendor)	
PIA - 23	Data Feed Service, piafrmcdc	7/26/2024	This is an invalid citation. Please refer to Records Control Schedules | National Archives HHS/CDC for an updated list of CDC's Record Control Schedules.	
PIA - 15	Data Feed Service, piafrmcdc	8/13/2024	Is there contact information that does not name a particular person, but possibly an office or team?	
PIA - 1	BLAND, CRYSTAL	9/20/2024	On the next iteration of the PTA, please update the following: Please provide POC and URL (if applicable). PTA-5A: Please respond "Yes."	

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:	10/2/2024 12:02 AM	**History Log:**	**View History Log**