Privacy Impact Assessment (PIA): CDC - BDSTEPS/CHDKIDS - QTR2 - 2024 - CDC8325435

Created Date: 7/11/2024 4:01 PM Last Updated: 8/7/2024 4:01 PM

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 - BDSTEPS/CHDKIDS - QTR2 - 2024 - CDC8325435	**PIA ID:**	2006403
Name of Component:	CDC - BDSTEPS/CHDKIDS	**Name of ATO Boundary:**	BDSTEPS/CHDKIDS
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	48
Submission Status:	Re-Submitted	**Submit Date:**	7/24/2024
Next Assessment Date:	08/07/2027	**Expiration Date:**	8/7/2027
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8325435
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.	Upgrade to new hardware and deployed new software. Moved BD-STEPS audit logging capabilities from the Elastic Stack (ELK) environment to the Security Operations Center (SOC)
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 purpose of BD-STEPS is to identify modifiable maternal exposures in early pregnancy that may increase the risk for having a pregnancy affected by certain major, structural birth defects. Mothers of the case infants and mothers of randomly selected live born control infants will be contacted and invited to participate in a maternal interview covering multiple topics. The BD-STEPS interview will focus on the key areas of: (1) diabetes, obesity, and physical activity; (2) other chronic maternal medical conditions; (3) infertility; and (4) medication use.
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.	Data collected during interviews will focus on the subject's experiences during her pregnancy and exposures to possible risk factors. The system contains health research data such as chronic conditions, medications used during pregnancy, baby's estimated delivery date, interview responses and mother's experiences during her pregnancy and exposures to possible risk factors. In order to conduct the study activities, the system maintains contact information for the purpose of mailing study related materials and calling study subjects for interviews. The system also contains contact information (name, phone number, email, and mailing address) for mothers of infants with a date of birth, or estimated date of birth for unborn babies, or pregnancy terminations, on or after September 1, 2014, in each of the study centers. BD-STEPS system users are required to have unique identification and authentication. BD-STEPS username and password with additional two-factor (2FA) authentication from Duo.
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.	Information collected via surveys is used for study analysis to identify modifiable maternal exposures in early pregnancy that may increase the risk for having a pregnancy affected by certain major, structural birth defects. PII is required for the interviewing contractor to contact, recruit, and interview sampled respondents. Username and passwords are required for system administrators requiring access to the BD-STEPS system to perform maintenance. Username and passwords are also required by researchers and call center administrators to access interviewing software and perform analysis.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
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)?	Yes
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.	The application is used to store subject's contact information like name, date of birth, email address, phone number and mailing address and to manage contact attempts to subjects. The application is also used for overall sample management at Abt Global and communicating the status of study subjects to individual CBDRPs. The application is only accessed by authorized Abt Global staff, and authorized CBDRPs staff. To access the application, users are required to enter username, password, and MFA.
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 Phone numbers Date of Birth Mailing Address
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.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	PII is required for the interviewing contractor to contact, recruit and interview sampled respondents. Participant user ID's and passwords are not collected. Username and passwords are required for system administrators requiring access to the Birth Defects Study To Evaluate Pregnancy exposureS (BD-STEPS) system to perform maintenance. Username and passwords are also required by researchers and call center administrators to access interviewing software and perform analysis.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	N/A
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	N/A
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	N/A

PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Public Health Service Act, Section 301, "Research and Investigation," (42 U.S.C. 241)
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Name, Date of Birth
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.	09-20-0136, "Epidemiologic Studies and Surveillance of Disease Problems"
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Government Sources State/Local/Tribal Non-Government Sources Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	OMB# 0920-0010
PIA - 10B:	Identify the OMB information collection approval number expiration date.	2/23/2023
PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A
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 State or Local Agency/Agencies Within HHS
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Datafile might be used for further research purposes within Department Health and Human Services (HHS). The vendor will share PII (i.e.., updated contact information) with State Agencies, so that the State Agencies have the most up-to-date contact information for their study mailings and other future contacts with respondents. PII is shared with to the vendor to conduct research and analysis.
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)).	Data Use And Security Agreement (DUA) have been signed between the vendor and 6 of the 7 study centers. CDC is the lead for the 7th study center, therefore no DUA is required. The DUA allows each Center to share PII with the vendor; The vendor to contact and collect data from each Center's study participants; and the vendor to share de-identified data with CDC.

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.	The data will be shared outside of CDC, the vendor, and the other participating study centers. In the event that an individual requests data from this system, CDC will account for the disclosure. According to the DUA, the parties agree that any data provided under this Agreement, along with any derivative files, can only be retained for the duration of the Agreement. At its conclusion, the Data Recipient must either return or destroy all original and derivative data files, following the specified guidelines. Any data stored in long-term storage must be destroyed within 13 months post-destruction date, using industry best practices, and must be certified in writing via a "Certificate of Destruction." The Data Recipient is also required to implement appropriate safeguards to protect the data, ensuring access is limited based on need-to-know principles and using secured storage and encryption for transmission. Additionally, authorized representatives from the Data Provider will have the right to inspect the Data Recipient's premises to verify compliance with the Agreement. The Data Recipient is responsible for ensuring that any agents or subcontractors adhere to the same restrictions. Any unauthorized disclosure of data must be reported to the Data Provider immediately. Both Parties recognize that certain personal, health, and financial data are subject to governmental regulations, which carry penalties for misuse. By signing this Agreement, the Data Recipient acknowledges these obligations and the potential penalties for violations, affirming their authority to commit to these terms.
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.	Voluntary
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.	The vendor receives PII from each Center. This PII is required in order for the vendor to make initial contact with participants. Participants can opt-out at any time thereafter. If participants request that any of their data be removed from the study, they are advised to contact their local study Center.
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.	If major system changes occur that require re-consenting study participants, the vendor will use the last available contact information to attempt to reach study participants. If the contact information is no longer valid, the vendor will use established tracing procedures to attempt to find updated contact information. Once the vendor reaches a study participant, the vendor staff will re-consent the participant as appropriate.

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.	Before the vendor contacts any study participants by telephone, participants are sent an advance packet by each study Center. The advance packet includes a Rights of Research Subjects flyer, which directs participants to contact the CDC Human Research Protection Helpline with any concerns about their rights as study subjects. At the start of each interview, vendor staff advise study participants to contact their study Center if they have any concerns about the study. Vendor staff also direct study participants to either the local study Center IRB (Institutional Review Board) or CDC's IRB (depending on the Center) if they have any questions about their rights as a study subject. The vendor will work in consultation with each of the 7 Study Centers when a subject requests to have their study data removed or changed. Subjects are provided several pieces of contact information: The vendor toll-free number and email address: questions@bdsteps.org at 1-888-743-7324 Their center's project manager's name and phone number The local center's IRB contact information: • AR: University of Arkansas for Medical Sciences Institutional Review Board Office, 1-501-686-5667 or irb@uams.edu • CA: Committee for the Protection of Human Subjects, California Health and Human Services Agency, at 1-916-326-3660 or cphs-mail@oshpd.ca • IA: Human Subjects Office at 1-319-335-6564 or irb@uiowa.edu • MA: Massachusetts Department of Public Health Institutional Review Board Chair at 1-617-624-5621 • NY: New York State Department of Health Institutional Review Board 1-518-474-8539 • CDC's IRB: Office of the Deputy Associate Director for Science for CDC at 1-800-584-8814 If a subject contacts the vendor with a concern, the vendor notifies the Center and CDC, who conduct an investigation and reach a resolution, in consultation with the vendor. The Center and CDC notify the vendor if a subject's PII is to be removed or corrected in study databases.

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.	The vendor staff confirm that accuracy of PII at each contact with the study subject, including during the interview survey and when sending follow-up mailings (reminder and thank you letters). The PII will not be checked for regular integrity, availability, accuracy, or relevancy because the PII will not be retained or linked back to the individual. As with all data that is not PII, it will be checked for outliers and other potential inaccuracies due to improper entry.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators 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.	Users require access to information to perform analysis and research. Administrators require access to the system for timely system maintenance and troubleshooting. Indirect contractors require access to the information to perform analysis and research.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	CDC will approve all users, including contractors, who request access to the data based on the least privileged model. Within CDC, the CDC project team reviews any access request to the data. CDC has approved the contractor to access the data. The vendor requires that any user (or subcontractor) must be approved by the project lead before accessing the data. The project lead also provides approval for administrators access to the BD-STEPS data.
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.	Only authorized users are allowed access PII. Access to PII is removed when a user leaves the organization or no longer requires access to do their job. External users cannot access PII. BD-STEPS restricts access to PII using privileges assigned to system accounts and uses least privilege model within the survey application's tables and views. Standard internal users that are interviewers can only view information on the cases that are assigned to them. They only have access to the PII for their cases. Access to this information is required for the interviewer to complete the survey. If a user is identified as an Administrator, then their system account will receive the appropriate privileges to perform account management duties.

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.	All personnel with access to the system receive general security awareness training, and personnel with privileged access or significant information security roles receive additional role-based security training before they receive access to the system, when required by system changes, and annually thereafter.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	The vendor provides Health Insurance Portability and Accountability ACT (HIPAA), Data Security Plan, Privacy, and Incident Response training. These trainings are conducted at least once a year and prior to authorizing access to the system. Study-specific training for interviewers on how to conduct the survey interviewing is also conducted by the study survey lead.
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 maintained based on CDC's Scientific and Research Project Records Control Schedule (N1-422-09-01). The PII is not needed for long term retention of the data and will not be archived. The vendor retains documents as required by CDC. By default, data is stored by the vendor for 5 years. Data security plans are developed as appropriate and define the data destruction timelines for the project. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. CDC will retain the records for 20 years; or longer if further study is needed.

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: BD-STEPS follows vendor policies and procedures for access control, personnel management, system management, incident response and contingency planning. The vendor provides general security training and awareness to all its employees at least annually plus additional role-based security for privileged users. Technical controls: All user accounts have strong password requirements, and all devices that store the data utilize FIPS 140-2 full device encryption. All access to the system requires multifactor authentication using Duo. To protect the files, Microsoft Windows Active Directory controls folder permissions through discretionary access control. Regular scanning for vulnerabilities on BD-STEPS is performed at least every month using Tenable.io. All data is encrypted at rest using full disk encryption on the Storage Area Network and in transit. Physical Controls: The data is physically stored in the vendor's office facility that is secured using key card access and the servers are within a separate secure server room with restricted access. The facility has cameras, alarms, and fire suppression systems. BD-STEPS follows the vendor Physical and Environmental Protection Policy that ensures all employees are issued a badge prior to accessing secure areas.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	7/25/2024
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:**	7/25/2024
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	7/29/2024
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 7/29/2024 This PIA is ready for SAOP review and approval. Per CDC email (see Supporting Documentation) confirmed that "CBDRPS " stands for Centers for Birth Defects Research and Prevention (CBDRP). The remaining comments are minor and can be updated in the next iteration of the PTA/PIA.	**Agency Privacy Analyst Days Open:**	4

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Per CDC email (see Supporting Documentation) confirmed that "CBDRPS " stands for Centers for Birth Defects Research and Prevention (CBDRP). The remaining comments are minor and can be updated in the next iteration of the PTA/PIA.	**SAOP Review Date:**	8/7/2024
		SAOP Days Open:	9

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Re_ CDC - BD-STEPS - QTR2 - 2024 - CDC8325435.pdf	218835	.pdf	7/29/2024 9:42 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 11D	Data Feed Service, piafrmcdc	7/11/2024	Please reference the procedures listed in the DUA.	
PIA - 22	Data Feed Service, piafrmcdc	7/11/2024	Please define all acronyms upon first use.	
PIA - 11D	Data Feed Service, piafrmcdc	7/16/2024	The reader is not expected to have access to the DUA. Please summarize the procedures here.	
PIA - 11D	Data Feed Service, piafrmcdc	7/23/2024	The first sentence contradicts 11-A which indicates the PII will be shared.	
PIA - 11C	Data Feed Service, piafrmcdc	7/24/2024	Remove "Abt Global" from this PIA in all responses here and below.	
PIA - 15	BLAND, CRYSTAL	7/26/2024	Remove bullets as they're not 508 compliance.	
PIA - 1	BLAND, CRYSTAL	7/26/2024	On the next iteration of the PTA: Please spell out the following acronyms the first time used, "BD-STEPS," "CBDRPS," and "MFA."	

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:	8/7/2024 4:01 PM	**History Log:**	View History Log