Privacy Impact Assessment (PIA): CDC - NCHS-RSS - QTR2 - 2023 - CDC6744994

Created Date: 6/16/2023 10:36 AM Last Updated: 1/15/2025 3:01 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 - NCHS-RSS - QTR2 - 2023 - CDC6744994	**PIA ID:**	1671778
Name of Component:	CDC - NCHS Rapid Surveys System	**Name of ATO Boundary:**	NCHS Rapid Surveys System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	374
Submission Status:	Re-Submitted	**Submit Date:**	8/23/2023
Next Assessment Date:	05/13/2027	**Expiration Date:**	5/13/2027
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC6744994
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)?	No
4:	ATO Date or Planned ATO Date.	9/1/2023
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.	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?	Contractor

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 Centre for Disease Control and Prevention's (CDC) National Center for Health Statistics (NCHS) Rapid Surveys System (RSS) is a platform to provide fast, reliable, actionable data, of known quality, to inform public health experts, government officials, and communities. The National Center for Health Statistics (NCHS) Rapid Surveys System's (RSS) purpose is : (1) to provide CDC and other partners with time-sensitive data of known quality about emerging and priority health concerns, (2) to use these data collections to continue NCHS's learning and evaluation of the quality of public health estimates generated from commercial online panels, and (3) to improve methods to appropriately communicate the fitness for use of public health estimates generated from commercial online panels. National Center for Health Statistics (NCHS) Rapid Surveys System (RSS) contracts with a third-party vendor, which incorporates proprietary statistical collection analyzes tools and methods. NCHS RSS relies upon survey panels that consist of respondents contracted by the vendor to participate in quickly developed/deployed (i.e., time-sensitive) information collection activities in support of NCHS mission. The vendor survey panel solution is the same commercial solution used for all clients government and non-government. NCHS RSS facilitates the development of innovative methods for estimation and increasing representativeness as well as provides transparent information about data quality and limitations.
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.	NCHS RSS will process and/or maintain: (1) health and healthcare-related survey response data (gender identity, sexual orientation, income level, education level, e.g. attained high school diploma, and general medical survey responses, e.g. "Have you EVER HAD a mammogram?"). Vendor destroys data once it is transferred to NCHS, no less than quarterly. NCHS RSS authenticates via it own Active Directory (AD) that falls within the NCHS RSS security authorization boundary.
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	

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.	NCHS RSS will process and/or maintain: (1) health and healthcare-related survey response data (gender identity, sexual orientation, income level, education level, e.g. attained high school diploma, and general medical survey responses, e.g. "Have you EVER HAD a mammogram?"). The single category of individual from which information is collected is survey panel respondents contracted by the vendor. Health and healthcare-related survey response data is collected from these individuals in order to evaluate feasibility of utilizing commercial web survey panels to inform public health decisions such as policy and epidemiological tracking.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	
PTA - 8:	Does the system include a website or online application?	No
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	
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.	
PTA - 10:	Does the website have a posted privacy notice?	
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	
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?	
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?	
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.	Employment Status Other - Free text Field - Gender identity, sexual orientation, income level, education level (not records), general medical questions (not records)
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
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?	Indirect PII are collected from administered surveys to perform calibration, weighting, and benchmarking for analysis and surveillance of public health.
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.	Section 308(d) of the Public Health Service Act, 42 U.S.C. 242m(d) Confidential Information Protection and Statistical Efficiency Act or CIPSEA, Citation: 44 U.S.C. 3561-3583
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 Other
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	0920-0214

PIA - 10B:	Identify the OMB information collection approval number expiration date.	6/30/2026
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?	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.	Individuals whose data is collected are survey respondents; respondents can opt-out at any time by withdrawing from the survey panel.
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.	Individuals whose data is maintained in the system have entered into a contract with the vendor wherein they consent to the storage of this data. In the unlikely event of a major change to the system, individuals cannot be notified because the system is designed to only store anonymized survey response data. It is therefore impossible to identify any particular individual from their data.
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.	The vendor's Data Protection Officer (Address: 222 West Adams St, Attn. Data Protection Officer, Chicago, IL 60606) would be the point of contact for any such concern regarding inappropriate use or disclosure of PII. Individuals cannot be notified specifically because the system is designed to only store anonymized survey response data. It is therefore impossible to identify any particular individual from their data; however, the vendor's Data Protection Officer would send a generic breach notification to all panelists (i.e., individuals) in the event of any widespread system compromise.
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.	There is an annual review that is conducted by Division of Health Interview Surveys (DHIS) staff to ensure integrity and availability of data systems containing this system's PII. DHIS staff undergoes annual training to further assure integrity and confidentiality of the system's data. National Center for Health Statistics Rapid Surveys System (NCHS RSS) relies on survey respondents to be accurate in their responses; PII contained in the system is exclusively anonymized survey response data and as such cannot change over time or be traced back to a respondent to verify accuracy.

PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv 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 and administrators are all contractors. Users – project staff must access the PII to perform routine data processing as part of vendor's contractual duties for National Center for Health Statistics Rapid Surveys System (NCHS RSS). Administrators – administrators have access to PII as a routine consequence of their general, elevated, system access.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	National Center for Health Statistics Rapid Surveys System (NCHS RSS) utilizes role-based access control (RBAC) to determine appropriate user access. Roles for user level can be overall for managers and senior researchers to project based, as the user's job function requires. All newly provided access, changes in access, addition of roles, or changes to the roles require approval by project management.
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.	The system relies on its own Active Directory, and multi-factor authentication (MFA), to provide strict role-based access control (RBAC).
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.	Users working on National Center for Health Statistics Rapid Surveys System (NCHS RSS) are required to take annual security awareness training, sign a Designated Agent Agreement, an Affidavit of Nondisclosure, and complete CDC's Confidential Information Protection and Statistical Efficiency Act (CIPSEA)-specific awareness training. Further, all users must annually sign Rules of Behavior (RoB). Failure to maintain Designated Agent status or to sign the RoB annually will result in account suspension until completed.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users of the system are required to take and adhere to CDC's Confidential Information Protection and Statistical Efficiency Act (CIPSEA) training annually. In addition, the users receive the following: 1. Annual Overview of Records Management: Every user has to sign an annual Non-Disclosure Affidavit 2. Contractor employees annually sign CDC/NHCS/DHIS Non-Disclosure Agreement 3. Annual Designated Agent 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).	Contract requires vendor to destroy data upon delivery to National Center for Health Statistics (NCHS), which occurs at least quarterly. Once data has been transferred to NCHS, survey output data, including analysis and reports, are retained according to Records Control Schedule N1-442-09-1-1a which specifies data should be retained permanently. Vendor adheres to NIST-800-88 sanitization guidance for destruction procedures including clearing and purging via the tool Darik's Boot and Nuke (DBAN) configured to use "Wipe method of US DoD", 7 passes, and wipe verification and destruction via shredding of hard copies and decommissioned hard disks.
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: documented policies and procedures and non-disclosure agreements that project staff agree to adhere to upon project onboarding and annually thereafter, annual security awareness training, Role-Based training, minimum necessary Role-Based access, monitoring of access logs and user activities, established data disposition procedures, periodic correspondence with CDC staff to reinforce confidentiality regulations, guidelines, and procedures; background investigations. Technical controls: access restrictions based on least privilege and need to know, Role-Based access managed by NCHS RSS AD and multi-factor authentication (MFA), virus/malicious code detection software, firewalls, virtual private network, intrusion detection system, database backups, and encryption is utilized to protect some database data elements. Physical controls: building security guards, identification badges, key cards, closed circuit TV, and locked offices.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	8/23/2023
Privacy Analyst Comments:	The Center has provided documents to address the SOP comments on 10A and 10C.	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker.	**SOP Review Date:**	8/29/2023
		SOP Days Open:	6

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	2/20/2024
Agency Privacy Analyst Review Comments:	2/20/2024: Reviewer: Nestor Villafuerte- This PIA is ready for SAOP review and approval. 7/31/2023: Reviewer: Giselle Sayon Please review comment and update accordingly. PIA-9: Per PTA-8 and PTA-14 there are no website, online applications, or mobile apps tied to this system. So how does CDC collect the information directly from the individuals online? I thought the contracted vendor collects the data and provides it to CDC.	**Agency Privacy Analyst Days Open:**	175

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	
SAOP Comments:	Approved on behalf of Bridget Guenther	**SAOP Review Date:**	5/13/2024
		SAOP Days Open:	83

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
NCHS-RSS _PIA_bl 6-22-2023_PIM_GS_jl.rtf	809744	.rtf	7/31/2023 8:08 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	6/8/2023	What kind of PHI is within the medical records?	
PIA - 1	Data Feed Service, piafrmcdc	6/12/2023	Met with the Center on 6/12/23 and confirmed that no PHI will be collected.	
PIA - 9	BLAND, CRYSTAL	7/31/2023	Per PTA-8 and PTA-14 there are no website, online applications, or mobile apps tied to this system. So how does CDC collect the information directly from the individuals online? I thought the contracted vendor collects the data and provides it to CDC.	
PIA - 10A	Data Feed Service, piafrmcdc	8/15/2023	Was the OMB number granted?	
PIA - 10C	Data Feed Service, piafrmcdc	8/15/2023	Was the OMB number granted?	

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:	1/15/2025 3:01 PM	**History Log:**	View History Log