Privacy Impact Assessment (PIA): CDC - NHANES - QTR2 - 2024 - CDC8270759

Created Date: 5/17/2024 4:02 PM Last Updated: 10/1/2024 8:01 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 - NHANES - QTR2 - 2024 - CDC8270759	**PIA ID:**	1830026
Name of Component:	CDC - National Health and Nutrition Examination Survey	**Name of ATO Boundary:**	National Health and Nutrition Examination Survey
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	140
Submission Status:	Re-Submitted	**Submit Date:**	9/3/2024
Next Assessment Date:	10/01/2027	**Expiration Date:**	10/1/2027
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8270759
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.	8/19/2021
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.	
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The contractor managing the system has changed.
PTA - 3:	Is the data contained in the system owned by the agency or 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 NHANES survey combines interviews and physical examination data. The purpose of the National Health and Nutrition Examination Survey (NHANES) system is to collect, analyze and disseminate data on the health of Americans. All major diseases, risk factors and behaviors, environmental exposures, and relationship between diet/health/nutrition are assessed. NHANES data is used to measure the prevalence of numerous chronic diseases and risk factors, to measure exposure to hundreds of environmental chemicals, and to measure the nutritional intake of U.S. population.

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.	The NHANES system collects, analyzes and disseminates data on the health of Americans. All major diseases, risk factors and behaviors, environmental exposures, and relationship between diet/health/nutrition are assessed. The system collects and processes health and nutritional information annually from about 5,000 adults and children in the United States. PII is collected to allow future contact of a survey participant to report results of medical tests and for future longitudinal research both passive and active. NHANES collects the following types of PII: Social Security Number; Name; Date of Birth; Mother's Maiden Name; E-Mail Address; Mailing Address; Phone Numbers; Military Status; Employment Status; Foreign Activities; Medical Notes, Biometric Identifiers, Photographic Identifiers and Medicare Health Insurance Claim Number.
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card HHS Username Password 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.	The various types of information are collected during the survey to produce impersonalized data on the status of health of the population of the United States. The PII data is collected to allow future contact with a survey participant to report results of medical tests and for future longitudinal research both passive and active. PII (i.e., Social Security Number; Name; Date of Birth; Mother's Maiden Name; E-Mail Address; Mailing Address; Phone Numbers; Military Status; Employment Status; Foreign Activities; Medical Notes, Biometric Identifiers, Photographic Identifiers and Medicare Health Insurance Claim Number) can be used by collaborators or researchers under a very strict control in the NCHS Research Data Center (RDC). At the RDC, survey data is used in a controlled environment allowing only aggregated information to be disseminated from the RDC.
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 purpose of the following website https://www.cdc.gov/nchs/nhanes/ is for general public to review NHANES public data. General Public can access this website via the URL and no log in is required. The purpose of the following website https://myhealthsurveyportal.cdc.gov is for registration of Survey participants. The survey participant will have access to the website using login with Multi Factor Authentication (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?	Yes
PTA - 13A:	Does the website collect PII from children under the age thirteen?	No
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?	Yes
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.	Social Security Number Name Mother Maiden Name Email Address Phone numbers Military Status Foreign Activities Date of Birth Photographic Identifiers Biometric Identifiers Mailing Address Employment Status Other - Free text Field - Medical Notes and Medicare Helth Insurance Claim Number.
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?	Personally Identifiable Information (PII) is collected to allow future contact of a survey participant to report results of medical tests and for future longitudinal research both passive and active.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Personally Identifiable Information (PII) can be used by collaborators or researchers under a very strict control in the National Center for Health Statistics (NCHS) Research Data Center (RDC). At the RDC, survey data is used in a controlled environment allowing only aggregated information to be disseminated from the RDC.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Social Security Number (SSN) is collected from survey participants who have consented to having their survey data linked with other health records and is to be used to ensure the accuracy and quality of the data linkage.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	The legal authority is EXECUTIVE ORDER 9397 NUMBERING SYSTEM FOR FEDERAL ACCOUNTS RELATING TO INDIVIDUAL PERSONS.

PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	The legal authorities governing information use and disclosure are granted in: 1. Public Health Service Act, Title 42, US Code, Paragraph 242k - National Center for Health Statistics; 2. Food Quality Protection Act of 1996 (P.L. 104-170), Title III - Data Collection Activities to Assure the Health of Infants and Children and Other Measures, SEC. 301; 3. Food, Conservation, and Energy Act of 2008 (P.L. 110-234), SEC. 4403. Joint Nutrition Monitoring and Related Research Activities; 4. Federal Food, Drug, and Cosmetic Act (21 USC 393) Title 21 - Food and Drugs, Chapter 9 - Federal Food, and Cosmetic Act - Subchapter IX - Miscellaneous - SEC. 393. Food and Drug Administration (21 USC 393)
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 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.	09-20-0164 "Health and Demographic Surveys 09-20-0164 "Health and Demographic Surveys Conducted in Probability Samples of the United States Population. HHS/CDC/NCHS."
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	Office of Management and Budget (OMB) information collection approval number 0920-0950
PIA - 10B:	Identify the OMB information collection approval number expiration date.	4/30/2025
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.	Participation in the study is voluntary and participants are asked to sign electronic or hardcopy consent documents prior to data collection. Each participant is given a detailed explanation on how their PII is going to be used. They are not obligated to give their real name, phone number, address, or any other PII collected.
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.	Should major changes occur in the future each individual would be re-contacted for consent to the changes. Written informed consent to collect data is obtained prior to data collection. The informed consent process includes information on how the information will be used or shared.
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.	In case of a complaint from an individual, a report is filed with the NCHS ERB (Ethics Review Board) and each case is reviewed individually. The "hot line" phone number for queries from the public is 1-800-223-8118. The NCHS ERB e-mail address is nchs-erb@cdc.gov. The NCHS Ethics Review Board is located at 3311 Toledo Road, Hyattsville, MD 20782.
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 DHANES Director and NCHS Confidentiality Officer. Also the annual training of NHANES staff is conducted to ensure integrity, availability, accuracy, and confidentiality of NHANES data.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors 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 run research work in NCHS RDC (Research Data Center) controlled environment only. Administrators do system and data maintenance. Developers develop applications, run static code scans, and provide application maintenance. Direct and indirect contractors collect data for the NHANES and run maintenance cycles.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role-based access to data by the system users ensures least privilege and accountability.
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.	Role-based access to Personally Identifiable Information (PII) data with the need-to-know principal method ensures least privilege with the minimum access to the only amount of information necessary to perform the job
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 Information Security Awareness Training (ISAT) Annual Overview of Records Management Every employee and contractor have to sign an annual Nondisclosure Affidavit Annual Designated Agent training
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users must complete the following required trainings: the CDC Annual Information Security Awareness Training (SAT), Annual Overview of Records Management, and Annual Designated Agent training in accordance with Confidential Information Protection and Statistical Efficiency Act (CIPSEA). Furthermore, every user must sign an annual Non-disclosure Affidavit.
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).	National Health and Nutrition Examination Survey (NHANES) data is kept indefinitely. If a survey participant would request that his or her Personally Identifiable Information (PII) information should be destroyed, the data containing specific Personally Identifiable Information (PII) will be removed from the database. Records Schedule Number: N1-442-09-1

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.	The Personally Identifiable Information (PII) in the system is secured using a layered approach with appropriate administrative, technical, and physical controls being implemented. ADMINISTRATIVE CONTROLS: Includes Administrative controls to educate system users of their responsibility to protect PII, legally bind them to do so and include: All employees and contractor personnel are required to sign CDC Rules of Behavior and non-disclosure agreements as a condition of employment; regular personnel screening as required by CDC; Annual mandatory CDC privacy and security awareness trainings, and records management training for all users; Annual System Security Assessment with review of all security controls, NHANES network and system architecture, and system/network security; Monthly system security reviews and analysis; Regular scheduled backups of data; Role based access to data ensures least privilege and accountability. TECHNICAL CONTROLS: Includes User identification; Passwords; Two Factor Authentication; Firewalls; Virtual private network (VPN) to access data; Data encryption; Intrusion detection system (IDS); Monthly and Weekly system security scans; Equipment failure monitoring and replacement/duplication. PHYSICAL CONTROLS: Physical controls include Security guards at the entrance point; ID badges; Key cards; Closed circuit TV (CCTV); Servers with PII data are locked in caged area inside access protected room; Two-factor authentication required for entry to Primary and Alternate Data Centers.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	9/3/2024
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:	14

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	9/20/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 9/20/2024 All comments have been address, this PIA is ready for SAOP review and approval. 7/2/2024 The PIA is being rejected for updates to PIA-6 and PIA-6A. Please update accordingly. PIA-6: The response to PIA-6 is insufficient and needs to be updated. Why is SSN necessary to allow future contact? The system collects the name, email address, date of birth, mailing address, mothers maiden name, etc., all of which would enable CDC to contact an individual or even track them down if they move to a new address. The response to PIA-6 needs to be specific to the SSN. Please update accordingly. PIA-6A: Please note that the OMB control number is not a legal authority. Please cite "E.O. 9397" in your response.	**Agency Privacy Analyst Days Open:**	3

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	10/1/2024
		SAOP Days Open:	11

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Re_ CDC - NHANES - QTR1 - 2024 - CDC7804373.pdf	266594	.pdf	7/2/2024 3:07 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 9	Data Feed Service, piafrmcdc	5/17/2024	Please select "non-government-members of the public"	
PIA - 18	Data Feed Service, piafrmcdc	6/26/2024	Are there any differing aspects between administrators and developers? Why do they have the exact same roles?	
PIA - 1	BLAND, CRYSTAL	7/2/2024	On the next iteration of the PTA: PTA-5A Please provide a response as this was left blank.	
PIA - 6A	BLAND, CRYSTAL	7/2/2024	Please note that the OMB control number is not a legal authority. Please cite "E.O. 9397" in your response.	
PIA - 6	BLAND, CRYSTAL	7/2/2024	The response to PIA-6 is insufficient and needs to be updated. Why is SSN necessary to allow future contact? The system collects the name, email address, date of birth, mailing address, mothers maiden name, etc., all of which would enable CDC to contact an individual or even track them down if they move to a new address. The response to PIA-6 needs to be specific to the SSN. Please update accordingly.	

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:	10/1/2024 8:01 PM	**History Log:**	View History Log