Privacy Impact Assessment (PIA): CDC - VCDB - QTR4 - 2023 - CDC7269329

Created Date: 9/9/2024 12:01 PM Last Updated: 10/1/2024 3:20 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 - VCDB - QTR4 - 2023 - CDC7269329	**PIA ID:**	2185778
Name of Component:	CDC - Vanderbilt CISA Database	**Name of ATO Boundary:**	Vanderbilt CISA Database
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	277
Submission Status:	Submitted	**Submit Date:**	9/6/2024
Next Assessment Date:	10/01/2027	**Expiration Date:**	10/1/2027
Office:		**OPDIV:**	CDC
Security Categorization:		**OpDiv PIA ID:**	CDC7269329
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.	The system facilitates communication between caregivers and vaccinology and vaccine experts that otherwise may not communicate at all or in a much less efficient way. In this way, it is primarily a public health service. However, through the systematic collection of data, these activities also constitute a research resource to the scientific community, through assessing adverse events, discussing pathogenesis, and archiving data for future exploration.

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 system collects and maintains and shares data as described below: The Certified Information Systems Auditor (CISA) Clinical Case Review Tracking Workspace: patient's name, date of birth, medical history, vaccines received, clinical adverse event following vaccination, physician's name and contact information, and other clinical information. The Vaccine Safety Adverse Event Reporting System (VAERS): subject's name, date of birth, name of city or state, clinical adverse event, vaccines received and other clinical information. The Research Study: subject's name, contact information, vaccine received, adverse events, and other clinical information. The system does not use user ID and passwords. The users authenticate with key fobs. The key fob generates a unique code every time the user logs in. This code is not stored.
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.	Data processed by the Certified Information Systems Auditor (CISA) Clinical Case Review Tracking Workspace includes patient's name, date of birth, medical history, vaccines received, clinical adverse event following vaccination, physician's name and contact information, and other clinical information. Data processed by the Vaccine Safety Adverse Event Reporting System (VAERS) includes subject's name, date of birth, name of city or state, clinical adverse event, vaccines received and other clinical information. Data processed by the Research Study: subject's name, contact information, vaccine received, adverse events, and other clinical information. Data listed above is used to facilitate the immunization safety related information to community providers who administer vaccines. The community providers conduct an electronic survey that they will use to report unusual reactions to vaccines. Data is also used by the public health nurse to follow up with the provider if necessary to gather additional information and to contact vaccine experts to gather advice and information that they will enter the system and communicate with the provider.
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?	
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.	The website is used to facilitate communication between caregivers and vaccinology and vaccine experts that otherwise may not communicate at all or in a much less efficient way. The CDC, Vanderbilt University Medical Center (VUMC) and other university and hospital members of the Certified Information Systems Auditor (CISA) have access to the website. These users authenticate with key fobs. The key fob generates a unique code every time the user logs in. This code is not stored.
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?	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?	
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Does Not Collect PII
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No

PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Date of Birth Mailing Address Medical Records Number Other - Free text Field - Medical Records (Non-PHI)
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Patients
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	201 - 500
PIA - 4:	For what primary purpose is the PII used?	The system uses PII to analyze adverse reaction to Vaccines.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	A secondary use of PII is to keep case records and prevent future adverse reactions to vaccines.
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); and Sections 304, 306 and 308(d) which discuss authority to maintain data and provide assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)).
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.	Records may be retrieved by name, date of birth, and medical record numbers.
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.	Epidemiologic Studies and Surveillance of Disease Problems. 09-20-0136
PIA - 9:	Identify the sources of PII in the system.	Government Sources Within the OPDIV Non-Government Sources Members of the Public Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	N/A. Vaccine safety task orders are exempt under the National Vaccine Act.

PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A. Vaccine safety task orders are exempt under the National Vaccine Act.
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.	For patients who do not wish for their PII to be released, the referring physician can either 1) completely redact the documents so that no PII is provided or 2) cancel the referral to the CISA clinical case review.
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 can contact the Vanderbilt University to get a list of individuals whose PII we have. The CDC can then contact the individuals from this list or have Vanderbilt contact them on the CDC's behalf.
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.	Individuals can resolve concerns by contacting the physician or health care facility where they were treated. This person or office can put the individual in contact with Public Health department that requested the PII. This person can then contact the Vanderbilt System Manager. Individuals can also use the CDC contact information listed on the SORN. The CDC can then contact the Vanderbilt System Manager.
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.	Prior to entering PII into the electronic database, the data that are collected are monitored by the director of quality assurance, at the Vanderbilt Vaccine Research Program. This will ensure data integrity and accuracy.
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
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 will have access to PII according to their role and authorization. Users may include authorized personnel from Vanderbilt, the CDC, or from other CISA members. System administrators will have limited ability to access to data, but may have access to data due to permissions required for their job function. These duties include, general system administration, managing and testing backups, or storage management. Developers will have a limited ability to access the data, but may have access to data as a result of having privileges related to perform their job functions, including software development, testing, and debugging. Indirect contractors administer the system. Indirect contractor system administrators will have limited ability to access to data but may have access to data due to permissions required for their job function. These duties include, general system administration, managing and testing backups, or storage management. Indirect contractor developers will have a limited ability to access the data but may have access to data as a result of having privileges related to perform their job functions, including software development, testing, and debugging.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The procedures for adding new users to the environment include identifying the users, ensuring that they are authorized to access the system, identifying what data they are authorized to access, and issuing the minimum level of privileges to the user so that they can perform all necessary functions and only access the data for which they are authorized. Access is role based included the following roles: Administrator, Vaccine Expert, Health Nurse, Community Provider, Clinical Immunization Safety Assessment (CISA) Partner.
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 methods for providing only the minimum amount of information to personnel as required for their job function are built into the system architecture which allows for separation of duties using role-based access controls. This is applied at multiple layers of the system, including the Research Electronic Data Capture (REDCAP) application, and the user workstation environments.
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.	According to contract, Vanderbilt personnel must annually complete CDC IT security and privacy awareness training course to meet this requirement.

PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Role-based security awareness training is available through the NIH's website: http://irtsectraining.nih.gov/ The role-based courses are: Securing Remote Computers, Privacy Awareness Course, FDCC Systems Administrator Training, HHS Information Security for Executives, HHS Information Security for Managers, HHS Information Security for IT Administrators.
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).	CDC Records Retention Schedule N1-442-09-1 and General Records Schedule 5.2. Maintain at least 6 years, but no longer than 10 years after the retirement of the system depending on upon program need for scientific, legal, or business reference then delete/destroy. Source documents for computer are disposed of when no longer needed by program officials. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate. 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.
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 administrative controls securing PII for the system include a system security plan, contingency plan, regular back up of files, user manuals, and least privilege access. Personnel are trained and aware of their responsibilities for protecting the information collected and maintained. Technical controls include user identification, dual-factor authentication, a dedicated fire wall, an intrusion detection system, and encryption for data both in transit, and at rest. Physical controls include a restricted access facility, identification badges, key cards, and video monitoring.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	9/9/2024
Privacy Analyst Comments:	OpDiv Analyst: Joshua Mosios (Contractor) Please see comments and reach out to pia@cdc.gov/icr-privacy@cdc.gov with any questions.	**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:	11

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 they provided the exported version of the PIA (see Supporting Documentation) to confirm responses for: PTA-5A: No PTA-8: Yes PTA-10: No PTA-12: No All comments have been 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:	PTA-5A is blank, and PTA-5B list username and password but per PTA-5 The system does not use user ID and passwords. The users authenticate with key fobs. PTA-8, PTA-10, and PTA-12 displays “Error." 9/24/2024 Per CDC email they provided the exported version of the PIA (see Supporting Documentation) to confirm responses for: PTA-5A: No PTA-8: Yes PTA-10: No PTA-12: No	**SAOP Review Date:**	10/1/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
CDC - VCDB - QTR4 - 2023 - CDC7269329.rtf	220786	.rtf	9/24/2024 2:12 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	9/9/2024	Please de-select "Medical Records (PHI)" and, in the free text field, write "Medical Records (Non-PHI)".	
PIA - 20	Data Feed Service, piafrmcdc	9/9/2024	Define REDCAP	
PIA - 1	BLAND, CRYSTAL	9/24/2024	PTA: Need Clarification PTA-5A is blank, and PTA-5B list username and password but per PTA-5 The system does not use user ID and passwords. The users authenticate with key fobs. PTA-8, PTA-10, and PTA-12 displays “Error."	

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 3:20 PM	**History Log:**	View History Log