Privacy Impact Assessment (PIA): CDC - PDDA - QTR2 - 2024 - CDC8208296

Created Date: 5/6/2024 12:01 PM Last Updated: 9/30/2024 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 - PDDA - QTR2 - 2024 - CDC8208296	**PIA ID:**	1821678
Name of Component:	CDC - Pathogen Discovery and Detection Application	**Name of ATO Boundary:**	Pathogen Discovery and Detection Application
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	30
Submission Status:	Re-Submitted	**Submit Date:**	5/13/2024
Next Assessment Date:	05/31/2027	**Expiration Date:**	5/31/2027
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8208296
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.	5/31/2024
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

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 Pathogen Discovery and Detection Application (PDDA) system is a Laboratory-Based system that is used to Track Specimen Information. PDDA Captures Inventory Information, Manage Test results gathered from Pathogen Discovery, and detection procedures applied to specimens for which a pathogen has not been identified by way of traditional pathogen detection methods. State and Local Public health laboratories send results of specimens to CDC for testing.

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.	PDDA system collects basic information pertaining to clinical specimens that are to be tested. Data of patient's specimen include Patient Name, Email Address, Phone Number, Ethnicity, Gender, Date of Birth, Mailing Address, Username and Password. Results of specimen are reported to other CDC labs. Data is stored as long as the center's needs require, used for future references sure as similar outbreaks.
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card 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.	PDDA collects batches of patient specimens, makes aliquots from those specimens, make extractions from those aliquots, and document testing results from samples. Patient name and date of birth is collected, and patient specimen test results are kept permanently. They are not shared with external systems. Test results are only delivered to the issuing authority or entity securely according to Health Insurance Portability and Accountability Act (HIPAA) standards. This data represents patient and specimen related information (patient name, mailing address, email address, phone number and date of birth). This system requires username/password for access, PIV credentials and Active Directory (AD) to access data. AD has its own PIA.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
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 collect data (in batches) of patient's specimens from Lab technicians of the Pathogen Discovery. The website is also used to provide a report of the specimen identifiers tested when applicable.
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 User Credentials Other - Free text Field - Gender, Ethnicity.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Patients
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	51 - 200
PIA - 4:	For what primary purpose is the PII used?	PII is used to track viral outbreaks
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	To track specimen sent for Testing

PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	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?	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 Email Government Sources State/Local/Tribal Foreign
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	Information is not collected directly from the public.
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.	State or Local Agency/Agencies
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Test results are shared with those Agencies who provided the source data.
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)).	Not Applicable
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.	CDC is not the source of direct collection of PII from patients.
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.	CDC does not have direct contact with most individuals whose PII is collected. The collection of PII is voluntary PII submission is voluntary therefore individuals who want to opt-out do so at point of specimen collection not have to provide PII.

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.	CDC does not have direct contact with individuals whose PII is collected. Those sources may have varying processes for notifying individuals.
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.	CDC does not collect data direct from patients. The CDC receives data from the Health and State department; therefore, individuals address all concerns with their respective Health and State department that collected the data.
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.	As part of annual operation analysis, the technical team reviews and keeps membership current after confirming with the subject matter experts (SME). This is ongoing activity but end of a year CDC staff double check. The technical team reviews reports to confirm no PII are present. On a regular basis, the team reminds the members and users verbally and via emails to follow CDC security practices for a moderate level system.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers
PIA - 17A:	Select the type of contractor.	
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: For the purpose of Data Analysis Administrators: For the purpose of Data Management Developers: For the purpose of System Maintenance
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role Based Access Controls are employed to determine which system users may access PII. All users must be approved by the Business Steward based on roles, duties and responsibilities.
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.	Encryption is implemented within the system. Users are only able to access the data they need based on the role based access control implemented within the system. The data is accessible by the authorized personnel only. The least privilege model is used to provide Read Only Access according to predefined roles.

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 CDC Security and Privacy Awareness training is provided.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Annual training provided CDC system users include Records Management Training, Role based 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).	Records are retained and disposed of in accordance with the CDC Records Control Schedule. Record copy of study reports are maintained in agency from two to three years in accordance with retention schedules. 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. Records are retained for 20 years; for longer periods if further study is needed. Records are retained in compliance with CDC Scientific and Research Projects Records Schedule NI-442-09-1, also known as Big Bucket.
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: Include the system having an approved Annual Assessment, an Authorization to Operate, System Security Plan, Contingency Plan, E-Authentication and Risk Assessment that help secured PII. Annual Security and Privacy Awareness and Records Management Training, Role-Based Training, and the proper use for information following the Rule of Behavior policy in accordance with applicable CDC policies is provided. PDDA administrators control and monitor user access, system log-in, enforce policies/procedures granting access on a need-to-know basis to meet responsibilities of protecting information collected and maintained, corporate incident response plans in place for retention and destruction of safe PII. Technical controls: PDDA users are authorized by system administrators, identify proofing require a Smart Card to gain access to the CDC network on user roles-based authorization. The system is monitored by the Network and IT security controls, administered by the Office of the Chief Information Officer (OCIO), Digital Services Office (DSO). Physical Control: PAAD system Data is secured using physical controls, the facility the system servers are hosted has multi-layers of protection includes guards, secure doors, requires card to entry, and CCTV monitor. PDDA users will have CDC or HHS Identification Badges clearance.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	5/15/2024
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:**	5/17/2024
		SOP Days Open:	4

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/23/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 5/23/2024 Per CDC email (see supporting Documentation) confirm that response for PTA-8 is "Yes" as it did not sync to OIS. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	6

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Per CDC email (see supporting Documentation) confirm that response for PTA-8 is "Yes" as it did not sync to OIS.	**SAOP Review Date:**	5/31/2024
		SAOP Days Open:	8

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Copy_of_PDDA Privacy_Impact_Assessment_PIA_bl (7).rtf	215261	.rtf	5/23/2024 3:47 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	5/6/2024	Please delete "username/password" and select "user credentials"	
PIA - 2	Data Feed Service, piafrmcdc	5/6/2024	Is information no longer collected from the public?	
PIA - 9	Data Feed Service, piafrmcdc	5/6/2024	Is PII no longer sourced from the public?	
PIA - 15	Data Feed Service, piafrmcdc	5/6/2024	There must be a mechanism for individuals to report potential issues for this system. A CDC help-desk, organization email account, or CSIRT would suffice.	
PIA - 1	Data Feed Service, piafrmcdc	9/30/2024	This System has been migrated within the OCIO ISB Infrastructure Services authorization boundary. All future updates should be made via the new Sub- Component application.	

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:	9/30/2024 8:01 PM	**History Log:**	View History Log