

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 - DLSDB - QTR1 - 2025 - CDC8639443	PIA ID:	2853075
Name of Component:	CDC - Dengue Laboratory Sample Database	Name of ATO Boundary:	Dengue Laboratory Sample Database
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	38
Submission Status:	Re-Submitted	Submit Date:	3/26/2025
Next Assessment Date:	N/A	Expiration Date:	4/17/2028
Office:		OPDIV:	CDC
Security Categorization:	Moderate	OpDiv PIA ID:	CDC8639443
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?		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.	N/A
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 Dengue Laboratory Samples Database System (DLSDB) is an internal client server system. DLSDB is used for surveillance of Dengue, Chikungunya, Zika, and other arbovirus occurrences in Puerto Rico and other locations.
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.	Patient and laboratory data on Dengue, Chikungunya, Zika, and other arboviruses. Patient data consists of Name, Mother's maiden name, email address, phone number, mailing address, medical records number, sex, and Country of birth. Laboratory data includes pathogens analysis and results.
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.	<p>The database contains patient information & laboratory results from the diagnostic lab. Patient data consists of Name, Mother's maiden name, email address, phone number, mailing address, medical records number, sex, and Country of birth. It searches for previous samples from patients, stores data on the samples, & stores results of epidemiological evaluations. The data is used for epidemiological analyses of disease activity in certain periods or locations by division scientists. Sample results are reported to the patients' health care provider.</p> <p>The use of a maps application will be used to get the longitude and latitude coordinates of patient's home address and the information will be added to the database and controlled by the program. Select fields of information will be extracted in Extensible Markup Language(XML) format and sent to internal low system ArboNet (ESC: 911). Similar data will be placed on the Encrypted File folders for Field staff.</p>
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?	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?	Yes
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	HHS

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.	Field data is collected via the Epi Info (ESC:71) mobile device or Research Electronic Data Capture (REDCap) mobile device or web application and uploaded via Application Programming Interface (API) after user login via SAMS Open Authorization (OAuth). Field data is collected with tablets, laptops, or desktops and transferred to the workstations for review. Some staff and contractors will collect data from the field and transmit the data back to DLSDB server via a web portal after connecting via SAMS API of Epi Info or REDCap. The data is transmitted via wireless access or over cell towers with encryption built in. Backups are written to a local tape device attached to the server.
PTA - 16:	Does the mobile application/ have a privacy notice?	Yes
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	No
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	Yes
PTA - 18:	Does the mobile application use measurement and customization technology?	No
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	Disease information is collected on the mobile application from the public in areas that are affected the most. Disease information is collected regarding tropical area viruses to COVID.
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	No
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	No
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?	No
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 Mother Maiden Name Email Address Phone numbers Mailing Address Medical Records Number Other - Free text Field - Sex, Country of Birth, Latitude - Longitude coordinates
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Patients 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?	The PII data is primarily used to track cases of Dengue, flu, Zika and other viruses to determine disease patterns.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	PII is also used to send epidemiological data to the patient's healthcare provider. Also, this data is used to track participants over a longer period of time.
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); sections 304, 306 and 308(d) which discuss authority to grant 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.	Data is retrieved by name.
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.	Government Sources State/Local/Tribal 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.	OMB Collection # 0920-1254
PIA - 10B:	Identify the OMB information collection approval number expiration date.	3/31/2026
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?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Private Sector State or Local Agency/Agencies

PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	<p>In case of a death, we verify that the Puerto Rico State Health Department knows about the case.</p> <p>Sample results are reported to the patient's health care provider because the health care provider sent the sample to us for processing. We are a Clinical Laboratory Improvement Amendments (CLIA) certified laboratory and can only report back to the healthcare provider that sent the sample to us.</p>
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)).	None
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 Principal Investigator (PI) for the study will receive the requests for disclosures of records from individuals (requesting their own records); and log them in a file cabinet (locked) in the data entry office at the San Juan campus. This request can come directly from the participant/patient or proxy (field staff, nurse epidemiologist, guardian/parent/tutor) and is directed to the PI for processing.
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.	<p>Individuals can choose not to write their address or their full name. We will nonetheless process the sample.</p> <p>Even if the patient opts-out, data elements are still required to be collected so the specimen itself can be tracked over time. Specimens with or without opting-in can both be tracked over time; however, the preference is to collect both specimen and sample together.</p>
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.	None. Individuals are given the choice not to provide their address or full name and it would be almost impossible to track all of them given the volume of records.

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.	If there is a PII incident where an individual believes their data has been compromised or is inaccurate, they would contact the CDC official specified in the SORN. In the case of a discrepancy, the submitter must provide identification and be able to reasonably identify the record and specify the information being contested, the reasons for requesting the correction, and the corrective action sought along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant. The CDC Official will work with the CDC testing laboratory to investigate and resolve the data security issue or discrepancy. CDC would facilitate the resolution based on the individual's request and report back to the individual following a successful resolution. Users can contact the PIs listed on the consent forms: Dengue Branch Chief at (787) 706-2399, or FDA Consumer Safety Officer at (787) 758-2000.
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.	Dengue Laboratory Sample Database (DLSDB) system implements various processes to ensure data integrity, availability, accuracy, and relevancy. This includes automated audits and reports (e.g., possible duplicate names, invalid addresses, missing gender, double-checking paper trails, etc.) to verify data accuracy and completeness; regular access reviews to maintain data availability, and stakeholder assessments to evaluate the relevance of the information collected. The lab also follows Clinical Laboratory Improvement Amendments (CLIA) and other quality assurance (QA)/quality control (QC) controls to ensure data is accurate. Any discrepancies identified during these reviews are promptly addressed through corrective actions, ensuring that the PII remains secure and up-to-date. Datasets are closed out on a yearly basis and only select staff can update these records.
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- Updating the system. Administrators- Updating and maintaining the system. Developers- Making changes to the system. Contractors-CDC direct contractors are used on this project for maintenance and user support and may incidentally view PII data to help troubleshoot user's problems in the system.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	<p>The system has logins that restrict the level of access to the data, and only those personnel determined to need access are granted credentials.</p> <p>Methods of access to the network is controlled through Active Directory, and access to the data on the Structured Query Language (SQL) server is controlled by Active Directory that restrict a user to either read only, Health Insurance Portability and Accountability Act (HIPAA) read only, or Read Write.</p>
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 has role based access to limit information accessibility based on least privileged.
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.	CDC Privacy and Security Awareness Training is administered on an annual basis.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Certain individuals are also required to undergo annual 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).	<p>All official records are transferred or destroyed based on CDC record management policies and practices. The following records schedules apply to the system:</p> <p>GENERAL RECORDS SCHEDULE 5.2: Intermediary records</p> <p>Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later</p>

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: Authorized Users: A database security package is implemented on CDC's mainframe computer to control unauthorized access to the system. Attempts to gain access by unauthorized individuals are automatically recorded and reviewed on a regular basis. Access is granted to only a limited number of physicians, scientists, statisticians, and designated support staff of the Centers for Disease Control and Prevention (CDC), or its contractors, as authorized by the system manager to accomplish the stated purposes for which the data in this system have been collected. Annual Privacy and Security Awareness Training is taken at least annually.

Physical Safeguards: Access to the CDC Atlanta facility where the mainframe computer is located is controlled by a cardkey system. Access to the computer room is controlled by a cardkey and security code (numeric keypad) system. Access to the data entry area is also controlled by a cardkey system. The hard copy records are kept in locked cabinets in locked rooms. The computer room is protected by an automatic sprinkler system, numerous automatic sensors (e.g., water, heat, smoke, etc.) are installed, and a proper mix of portable fire extinguishers is located throughout the computer room. The system is backed up on a nightly basis with copies of the files stored off site in a secure fireproof safe. Security guard service in buildings provides personnel screening of visitors.

Technical: The DLSDB system is behind firewalls and intrusion detection system to protect the data at rest. Encryption is in place to protect the data in transit as well as the database the data at rest. Protection for computerized records includes programmed verification of valid user identification code and password prior to logging on to the system, mandatory password changes, limited log-ins, virus protection, and user rights/file attribute restrictions. Password protection imposes user name and password log-in requirements to prevent unauthorized access. Each user name is assigned limited access rights to files and directories at varying levels to control file sharing.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	3/26/2025
Privacy Analyst Comments:	Updated per SOP Comments	Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	
SOP Comments:	Approved on behalf of Beverly Walker	SOP Review Date:	3/27/2025
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	4/18/2025
Agency Privacy Analyst Review Comments:	<p>Reviewer: Shanai Shobowale</p> <p>4/18/2025 All comments were addressed, this PIA is ready for SAOP review and approval.</p> <p>“Yes” the system has an ATO and the ATO Date is 1/20/2022.</p> <p>PTA-5A response: Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is - Active Directory (AD) is used and it has it's own security authorization boundary. External users uses Secure Access Management system (SAMS) that has it's own security boundary.</p>	Agency Privacy Analyst Days Open:	22

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:		SAOP Review Date:	4/18/2025
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
4-16-2025 EMAIL_Re_CDC - DLSDB - QTR1 - 2025 - CDC8639443.pdf	279891	.pdf	4/18/2025 7:14 AM	0
DLSDB_PIA_bl (16).rtf	252203	.rtf	4/18/2025 7:14 AM	0

Comments				
Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmc dc	3/12/2025	Phone number is included in the PTA but not here in the PIA.	
PIA - 8A	Data Feed Service, piafrmc dc	3/12/2025	Are direct identifiers actually used to retrieve record? Do not include those that may be used. Moreover, only include direct identifiers. For example, mother's maiden name is not a direct identifier.	
PIA - 8B	Data Feed Service, piafrmc dc	3/12/2025	If no direct identifiers are used to retrieve records in this system, a response here is n/a.	
PIA - 15	Data Feed Service, piafrmc dc	3/12/2025	Which official in the SORN should be contacted?	
PIA - 16	Data Feed Service, piafrmc dc	3/12/2025	Please describe the yearly process.	
PIA - 22	Data Feed Service, piafrmc dc	3/12/2025	How often?	
PIA - 24	Data Feed Service, piafrmc dc	3/12/2025	The controls listed under administrative controls appear to be technical controls. Are there any practices, policies or procedures in place to manage and reduce risks within the system in addition to training?	
PIA - 4	Data Feed Service, piafrmc dc	3/12/2025	Place the second purpose in PIA-5 under secondary purposes.	
PIA - 8A	Data Feed Service, piafrmc dc	3/26/2025	The goal of this question is to determine whether the Privacy Act applies. The Privacy Act does not include the term PII; it instead asks whether retrieval occurs by a name of an individual or some identifying number, symbol, or other identifying particular assigned to an individual. Within HHS, this type of information is called a "direct personal identifier." Direct Personal Identifier is information that is specific to a particular person such as biometric (fingerprint, hair, and eye color, etc.), date of birth, SSN, etc. Also, please note that data elements that may be used should not be listed. Only include direct personal identifiers that are actually used. If none are actually used, then the Privacy Act does not apply and the answer the previous question should be "no." Medical records numbers, age, and dob are not direct personal identifiers as on their own they do	

not directly identify an individual without additional information.

PIA - 15	Data Feed Service, piafrmcdc	3/26/2025	Please delete the names of individuals. Only include job titles.
PIA - 16	Data Feed Service, piafrmcdc	3/26/2025	Please define all acronyms upon first use.
PIA - 1	BLAND, CRYSTAL	4/18/2025	<p>“Yes” the system has an ATO and the ATO Date is 1/20/2022.</p> <p>PTA-5A response: Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is - Active Directory (AD) is used and it has it's own security authorization boundary. External users uses Secure Access Management system (SAMS) that has it's own security boundary.</p>

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	Is OpDiv Privacy Analyst Return ? :	0
Is Agency Privacy Analyst Approve ?:	1	Is SOP Return ?:	0
Is SAOP Approved?:	1	Is Agency Privacy Analyst Return ?:	0
Total Approved:	4	Is SAOP Return ?:	0
Total Approval Required:	4	Total Return:	0

Miscellaneous Fields

Last Updated:	4/18/2025 8:00 PM	History Log:	View History Log
----------------------	-------------------	---------------------	----------------------------------