Privacy Impact Assessment (PIA): CDC - IDPB Pathology - QTR3 - 2023 - CDC6795141

Created Date: 7/19/2023 11:55 AM Last Updated: 8/28/2024 3:28 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 - IDPB Pathology - QTR3 - 2023 - CDC6795141	**PIA ID:**	1679912
Name of Component:	CDC - CDC Pathology Report Information	**Name of ATO Boundary:**	CDC Pathology Report Information
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	407
Submission Status:	Submitted	**Submit Date:**	7/29/2024
Next Assessment Date:	08/28/2027	**Expiration Date:**	8/28/2027
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC6795141
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.	11/16/2024
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 Centers for Disease Control and Prevention CDC's Infectious Diseases Pathology Branch Pathology (IDPB) application is used to support the operational activities of the laboratory covering the full specimen lifecycle and support's the CDC's public health mission to diagnose, track, and report diseases, emerging infections and outbreaks in animal and human populations.

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 specimen and case information on animals and humans related to confirmed or suspected infectious pathogens. The data is used internally by CDC's Infectious Diseases Pathology Branch Pathology (IDPB) staff personnel. The information contains PII. The information is voluntary. All information is obtained at the State/Local/Tribal Health Department level. and manually uploaded into database. IDPB does not interact with any individual and therefore all responsibility for patient notification resides with the State. PII collected/stored permanently are patient name, date of birth, and medical record number. Other non-PII data collected/stored permanently for epidemiological, testing, and reporting purposes, include age, sex, specimen IDs, specimen description, state/country of origin, date received, clinical history, suspect infectious agents, submitters, test requests, diagnosis, test results, and date reported. Collection of data including PII is to diagnose, track, and report diseases, emerging infections and outbreaks in animal and human populations. Access to the IDPB Pathology system is based on a combination of **Personal Identity Verification** (PIV) card windows authentication and Role Based Access Controls managed by Digital Services Office - Infrastructure Services Branch (DSO ISB) database administration and only accessible to authorized IDPB personnel.
PTA - 5A:	Are user credentials used to access the system?	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
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.	The information collected and PII collected/stored permanently are patient name, date of birth, and medical record number. Other non-PII data collected/stored permanently for epidemiological, testing, and reporting purposes, include age, sex, specimen IDs, specimen description, state/country of origin, date received, clinical history, suspect infectious agents, submitters, test requests, diagnosis, test results, and date reported. Collection of data including PII is to diagnose, track, and report diseases, emerging infections and outbreaks in animal and human populations.
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?	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 Date of Birth Medical Records Number Other - Free text Field - Age, sex, State/Country Origin; Medical Records (not 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.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	To run, identify, track, and report tests on pathogens that have caused or are suspected to have caused illness or death (e.g., request test, diagnostics, Test Results, Dates Reported)
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	N/A
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	N/A
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	N/A
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Public Health Service Act, Section 301, "Research and Investigation," (42 U.S.C. 241)
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.	Government Sources State/Local/Tribal
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.	N/A. Information is not collected pursuant to the Paperwork Reduction Act (PRA): OMB Control Numbers are used for data collections subject to the Paperwork Reduction Act (PRA). PRA does not apply to data collections from government Agencies or instrumentalities. Information collected is from State/Local/Tribe government sources only.
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.	All information is collected at the State/Local/Tribal Health Department level. CDC does not interact with any individual and therefore all responsibility for patients to request to opt of PII data collection resides with the State/Local/Tribal.
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.	All information is collected from patients with consent at the State/Local/Tribal Health Department level. CDC does not interact with any individual and therefore all responsibility for patient consent to collect and notifications resides with the State/Local/Tribal.
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.	All information is collected from patients with consent at the State/Local/Tribal Health Department level. CDC does not interact with any individual and therefore all responsibility to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate resides with the State/Local/Tribal.
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.	The records are reviewed in accordance with the Physical and Procedural Safeguards, and Implementation Guidelines and Retention and Disposal policy. IDPB is a clinical laboratory, as such, it is under the jurisdiction of the Clinical Laboratory Improvement Amendment (CLIA) of 1988. CLIA's federal regulatory standards determine the relevancy of PII in the IDPB Pathology System.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users - Enter and update the system PII records Administrators - Administration over the system and correct issues with PII records as needed Contractors - CDC/HHS Credentialed contractors manage the database and trouble shoot the application

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	System Administrators in coordination with Business Steward will assign designated personnel for read/write to data fields. Least privilege, Role Based Access methods are used to allow those with specific need to PII to only access the minimum amount of information necessary to perform their job. The program first evaluates whether the individual has a need for access to the system. If the individual's manager determines that access to the system is required for the individual to perform their regular duties, they will make a request to the System Administrator. System Administrator will establish an account for the user access to IDPB by submitting access requests through Digital Service Office (DSO) Infrastructure Solutions Branch (ISB) Help Desk.
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.	Least privilege, Role Based Access methods are used to allow those with access to PII to only access the minimum amount of information necessary to perform their job. The system administrator is responsible for setting up the user access to the system based on the CDC user ID and the permissions assigned to it. Only one module of the IDPB Pathology system has all three PII fields visible; the Specimen Accessioning/Epidemiology module (used by the data accessioners and epidemiologists). Only one system generated PDF report that is reported to the case submitters has the three PII fields visible (Final Pathology Report module). None of the other seven team specific modules have the three PII fields visible.
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.	All CDC personnel are required to complete annual Security and Privacy Awareness Training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	All CDC personnel are required to complete annual Security and Privacy Awareness Training. All CDC employees who have access to PII/sensitive information are required to complete HHS/CDC 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 maintained in accordance with General Records Schedule (GRS) and comply with CDC Records Control Schedule (RCS). In accordance with GRS 5.2, final reports are created to document programmatic decisions, policies, and other related issues and are maintained permanently (CDC RCS, B-321, 2&4). Other input/output records and system data that may be required for follow-up are disposed of after 10 years. 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. In addition, electronic media is subject to zero-wipe pass (electronic destruction) methodology.
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: Completion of training requirements; risk analyses performed annually; branch management reviewing access requests and granting minimal amount of access. Technical controls: Users are authenticated and data secured using operating system and server security, administered by the local system administrator. PII data is encrypted at rest and in transits with access restricted to specific authorized users as required by HHS and CDC policy. Physical: The server is housed at a CDC Data Center with guards at all entrances to the campus and facilities, individual user access credentials are required for each non-public building , floor, and office. Closed Circuit TV is also used by the internal security guards to check for and grant access to authorized individuals.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	7/30/2024
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:**	8/7/2024
		SOP Days Open:	9

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	8/12/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 8/12/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	5

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	8/28/2024
		SAOP Days Open:	16

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	7/30/2024	Deselected Medical Records (PHI) and added Medical Records (Non-PHI) in the free text field.	

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:	8/28/2024 3:28 PM	**History Log:**	View History Log