Privacy Impact Assessment (PIA): CDC - DVBIDROS - QTR2 - 2023 - CDC6754042

Created Date: 7/19/2023 11:54 AM 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 - DVBIDROS - QTR2 - 2023 - CDC6754042	**PIA ID:**	1679907
Name of Component:	CDC - DVBID Reagent Ordering System	**Name of ATO Boundary:**	DVBID Reagent Ordering System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	379
Submission Status:	Re-Submitted	**Submit Date:**	4/10/2024
Next Assessment Date:	N/A	**Expiration Date:**	5/23/2027
Office:		**OPDIV:**	CDC
Security Categorization:	Low	**OpDiv PIA ID:**	CDC6754042
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Disposition
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.	7/10/2024
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.	DVBID Reagent Ordering System (DVBIDROS) serves as an ordering and inventory and control system for virus seeds, antigens, and antibodies for the Arbovirus Diseases branch. The data is used to track the amount of virus seeds, antigens and antibodies available at the storage facility and ordered by CDC or other public health agencies.

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 ordering information, including business contact information such as names, email addresses, and phone numbers for those persons authorized to initiate orders. The system uses User IDs and Passwords for non CDC users to authenticate to the system. The passwords are permanently stored in a database. CDC users are authenticated using Active Directory which is a separate system with its own PIA.
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.	DVBIDROS is a web-based ordering and inventory system of available virus seeds, antigens, and antibodies used by public health departments and researchers for reagent ordering. This system collects ordering information for reagents and business contact information on individuals. Collection of the business contact information is required which includes name, email address, phone number, and user credentials for external users. CDC staff require this information to verify the requestor's authorization and complete the ordering process. The system uses User IDs and Passwords for non CDC users to authenticate to the system. The passwords are permanently stored in a database. CDC users are authenticated using Active Directory which is a separate system with 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?	
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	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.	wwwn.cdc.gov/reagentorder
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 User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors
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?	Business contact information is required to register users in the system. User credentials are required for external users to register and access system.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	None
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?	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 Within the OPDIV
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 agencies, instrumentalities, or employees of the United States in their official capacities. Information collected is used for ordering inventory of regeants (e.g., virus seeds, antigens, and antibodies) in stock and is only collected and ordered from government agencies, instrumentalities, and U.S. Government employees. Voluntary commercial sales that require certain information to facilitate order and deliver products do not require PRA approval. This includes email or text subscriptions or alerts, such as email address and phone number, which facilitates orders. Additionally, information required for user account creation, such as email address, username, password, and geographic location do not require PRA approval. Therefore, the PRA does not apply and the requirement to obtain an OMB collection approval number is N/A. Reference: https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/inforeg/inforeg/memos/2014/appendix-data-search-tools-calculators.pdf https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/assets/inforeg/SocialMediaGuidance_04072010.pdf https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/inforeg/inforeg/memos/2014/web-based-interactive-technologies-data-search-tools-calculators-paperwork-reduction-act.pdf
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.	There is no provision to opt out. Individuals who want access must provide business contact information or the individual will not be able to register for and access the system.
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.	There is no process because this is a one-time collection to register users. Once registered, there is no further use by or within the system. There will be no major changes to the system since it is an inventory tracking and ordering system.
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 with concern about may contact the Business Steward by phone at 970-221-6415 or by mail at CDC MS P02 3156 Rampart Road, Ft. Collins, CO 80521 In lieu of a change of Business Steward, an individual can write to CDC Office of the Director Division of Vector-Borne Diseases 3156 Rampart Road, Ft. Collins, CO 80521
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 annual security assessments and certifications and accreditations of the application provide an over review of the systems security including Business Contact PII. The availability and intergrity of the data is ensured by the service level agreement between the system owner and the CDC information technology department. The system administrator performs database monitoring and maintenance when new data is entered into the system or changes are requested by the users Security controls are reviewed during the annual security self assessments and recertification process.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators
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.	System administrators have access to ensure proper role-based access and least privilege to the system.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	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 who will establish a role-based user access account for the user to access the system.

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 administrator is responsible for setting up the role-based user access to the system based on the configuration of the software application. The user does not have access to modify any of the configuration.
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.	Internal application users receive annual security training, to include privacy and awareness training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Persons with significant security responsibilities receive annual System 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).	Data is kept until no longer needed. GRS 5.2 Intermediary records. Records destroyed upon verification of the final document or file, or when no longer needed for business use, whichever is later. 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.	Administrative control is ensured by branch management reviewing access requests and granting minimal amount of access. Technical control is ensured by the system administrator granting user rights to the system based on role. Users are authenticated and data secured using operating system and server security, administered by the local system administrator. Physical control is ensured by, database server located behind two doors protected with card key locking systems, in a building with security guards, and locked doors.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	4/11/2024
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:**	4/29/2024
		SOP Days Open:	19

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/2/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 5-2-2024 Exported PIA (Supporting Doc.) confirm responses for PTA-7A and PTA-9. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	3

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Exported PIA (Supporting Doc.) confirm responses for PTA-7A and PTA-9. This PIA is ready for SAOP review and approval.	**SAOP Review Date:**	5/23/2024
		SAOP Days Open:	21

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Copy_of_DVBIDROS Privacy_Impact_Assessment_PIA_bl (7).rtf	942904	.rtf	5/2/2024 8:46 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 2	Data Feed Service, piafrmcdc	4/3/2024	Per the PTA, external users log in with passwords which are stored in the system. If that is the case, please select their relevant category.	
PIA - 17	Data Feed Service, piafrmcdc	4/3/2024	Please select "users" to include external registrants.	
PIA - 19	Data Feed Service, piafrmcdc	4/3/2024	Please describe an actual administrative procedure.	
PIA - 20	Data Feed Service, piafrmcdc	4/3/2024	The answer is more of an administrative procedure than technical. A technical procedure would be utilizing NIST encryption standards or implementing role-based access controls.	
PIA - 17	Data Feed Service, piafrmcdc	4/5/2024	Only Administrators have access to any PII and is only accessible internally. External users do not have access to PII other than their own username and password that they themselves enter to register and log in. To clarify, should I still check "Users" as instructed, or is the current selection for Administrators good?	
PIA - 2	Data Feed Service, piafrmcdc	4/5/2024	External / non-CDC Users are from federal, state, and local Health Agencies. The password / credentials stored in DSO managed database server is stored with irreversible hash. Additional relevant category added as requested.	
PIA - 10C	Data Feed Service, piafrmcdc	4/10/2024	Please clarify what this means.	
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