Privacy Impact Assessment (PIA): CDC - RIMS - QTR2 - 2025 - CDC8704777

Created Date: 4/30/2025 12:02 PM Last Updated: 5/30/2025 4:01 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 - RIMS - QTR2 - 2025 - CDC8704777	**PIA ID:**	3121485
Name of Component:	CDC - Reagent Inventory Management System	**Name of ATO Boundary:**	Reagent Inventory Management System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	31
Submission Status:	Re-Submitted	**Submit Date:**	5/12/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8704777
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.	6/2/2025
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.	
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	None - Archer missing PTA/PIA record
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 Reagent Inventory Management System (RIMS) is a part of The Division of Scientific Resources (DSR). RIMS an internal application built to allow DSR and its suppliers (CDC employees) real-time access to ordering and inventory information of reagents. The ordering of reagents is necessary to DSRs mission of providing CDC laboratories with storage, management, and distribution of reagents. RIMS owns all data collected and processed via the RIMS system.

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.	RIMS Collects name, work/mailing address, email address, and phone number of CDC users for the customer profiles. No external (non-CDC Users) use the system. The system does collect and use User IDs for log in purposes only. Users access the system using Personal Identity Verification (PIV) card, with authentication by the CDC Active Directory (AD). AD is a separate system with its own PIA.
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.	The Reagent Inventory Management System (RIMS) is an internal application developed by The Division of Scientific Resources (DSR) to facilitate real-time access to ordering and inventory information of reagents for CDC laboratories. The system is essential for DSR's mission of managing and distributing reagents effectively. RIMS owns all data collected and processed within the system. **Types of Information Collected:** RIMS collects various types of information categorized primarily into two groups: 1. **Business Contact Information:** 1. **Individuals Involved:** CDC employees and other business contacts (not patients). 2. **Data Collected:** This includes names, CDC User IDs, contact details (e.g., email addresses, phone numbers), and any other relevant business information necessary (e.g., work/mailing address) for managing orders and inventory. 2. **Controlled Unclassified Information (CUI):** 1. **Nature of Information:** This includes sensitive data related to biological select agents and toxins, categorized at a "Moderate" confidentiality impact level. 2. **Regulatory Compliance:** This information is regulated by the Federal Select Agent Program and is critical for ensuring compliance with federal guidelines. **System Processing and Modules:** RIMS consists of five modules that facilitate different aspects of data collection and processing: 1. **Login/Registration Module:** 1. Collects CDC User IDs during user registration and manages

		access through Active Directory with secure encryption methods. 2. **Customers Module:** 1. Allows users to manage customer profiles, which include business contact information. 3. **Orders Module:** 1. Role-based access for placing orders, ensuring that only authorized personnel can process orders for customers. 4. **Inventory Module:** 1. Users can view and maintain inventory data, including reagents and supplier information. 5. **Maintenance Module:** 1. Users can update their profile information and manage advanced system features, ensuring the integrity and accuracy of the data. **Data Collection Methods:** 1. Orders are received through various channels, including fax, email, and mail, and are manually entered into the RIMS system by authorized users. 2. The system allows for real-time reporting and data accessibility, enhancing the ability to analyze and respond to laboratory needs. **Types of Customers:** RIMS serves a diverse range of customers, primarily consisting of: 1. State and County public health laboratories 2. National and international universities 3. Public and private hospitals 4. Manufacturers and private laboratories 5. Other public health entities both domestically and internationally **Data Sharing and Reporting:** 1. RIMS generates reports that aid CDC statisticians in outbreak analysis and reporting capabilities. 2. Reports containing Controlled Unclassified Information are marked as “Sensitive But Unclassified” in accordance with CDC policy (CDC-IS-2005-02).
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?	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.	RIMS Inventory System Users are internal users who are verified via CDC Active Directory. There are five different modules: 1. Login/Registration: The Login/Registration module is where users go to register for access to the system. The website is used to register users. The system gathers the user's CDC User ID. After registration is approved, the application uses Active Directory with Kerberos AES 256 encryption for system access. Passwords are not stored or salted. Credentials are not cached. 2. Customers: The Customers Section module allows users to view, add, update, or delete customer information in real-time. Customers are Business Contacts (not patients) and the information maintained in the profile is categorized as Business Contact Information. 3. Orders: The Orders module is role based and allows users with the appropriate access to place orders for customers. 4. Inventory: The Inventory module allows certain user roles to view information on inventory (reagents, lots, reports), maintain inventory (add new items, edit/update/delete items, assemble kits, etc.), or maintain supplier information. 5. Maintenance: The Maintenance module allows users to update their profile information. Users are considered Business Contacts and the information maintained in the profile is categorized as Business Contact Information. Super users use this section to maintain advanced system features e.g. Security (Access and Reports), User Maintenance, Supplier Maintenance, and Lookup Tables. RIMS Inventory System Users access the information system through an internal web address, which Not Publicly Accessible.
PTA - 10:	Does the website have a posted privacy notice?	No
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 Mailing Address Other - Free text Field - User ID
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Below 50
PIA - 4:	For what primary purpose is the PII used?	The primary purpose of PII is to register system users.
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.	This information system is exempt from OMB review per the Paperwork Reduction Act (PRA). Information collected is for administrative purposes only (Internal Management/Operational Needs 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.	NA. The user can tell their supervisor they do not wish their Business Contact information used. However, not providing the contact information would mean the user cannot 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 in place to notify individuals that their personal information will be collected. All the users are CDC employees or contractors, and consent is a condition of employment and access to any CDC information 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 concerns about the use of their PII can contact the system Point of Contact previously identified in this PIA.

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 availability and integrity 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 user. 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.	Administrators: System Administrators have access to ensure proper role bases 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.	Only the system administrator(s) have access to the PII and only for maintenance activities, like adding/deleting users. The Business Steward or the designated Project Manager grants access to the Information System by assigning roles such as system administrator, developer, or contractor based on the user's job responsibilities and the principle of least privilege, ensuring that only those who require access to perform their duties are granted such permissions.
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 employs role based security controls. The System Administrator can limit access based on the users job function and role, employing the concept of least privilege.
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.	Application users receive annual Security and Privacy 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 manually entered (Input Data) is collected, and disposed of when no longer needed. These records are needed for administrative and research purposes Output Data: 1) Data generated from the RIMS Information System is in the form of Final Reports: In summary form, the findings and conclusions reached relative to scientific projects both with CDC and through Contractual arrangements 2) Reports for inventory and shipping information The retention for the output data is ten (10) years. These records are needed for administrative and research purposes System Data: System Data is created for research purposes that may be required for follow up or reference for a moderate period of time. The retention period for this data is ten (10) years. These follow the CDC Records Schedule: RCS, B-321
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 are ensured by branch management reviewing access requests and granting minimal amount of access. Role based controls are implemented. Technical controls are ensured by the system administrator granting user rights to the system based on roles. Users are authenticated and data secured using operating system and server security, administered by the local system administrator. Physical controls are ensured by database server located behind doors protected with card key locking systems.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	5/12/2025
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker.	**SOP Review Date:**	5/13/2025
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/21/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 5/21/2025 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	8

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Reviewer notes that PTA-2 failed to sync. Please select "Yes" for PTA-5a and mention AD in PTA-5b.	**SAOP Review Date:**	5/30/2025
		SAOP Days Open:	9

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	5/6/2025	The PTA states "The system does collect and use User IDs for log in purposes only." Then, the next paragraph there is a contradictory statement that a different system collects user credentials. Please clarify. Does User ID need to be included here? If not, remove the statement in the PTA.	
PIA - 23	Data Feed Service, piafrmcdc	5/6/2025	Please use complete sentences to make this information easier to understand and reduce the risk of misinterpretation. Does the citation at the end apply to all data types listed or just the last type listed?	
PIA - 24	Data Feed Service, piafrmcdc	5/6/2025	The sentence beginning with "Role based..." does not have a period at the end. I'd just like to confirm whether any information was mistakenly cut off? Is any information missing from the sentence? Is the sentence complete?	
PIA - 1	VILLAFUERTE, NESTOR	5/15/2025	Reviewer notes that PTA-2 failed to sync. Please select "Yes" for PTA-5a and mention AD in PTA-5b.	

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:	5/30/2025 4:01 PM	**History Log:**	View History Log