Privacy Impact Assessment (PIA): CDC - CoreOrder - QTR3 - 2024 - CDC8382350

Created Date: 7/29/2024 12:03 PM Last Updated: 8/22/2024 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 - CoreOrder - QTR3 - 2024 - CDC8382350	**PIA ID:**	2069965
Name of Component:	CDC - Core Order Web Based Ordering System	**Name of ATO Boundary:**	Core Order Web Based Ordering System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	29
Submission Status:	Re-Submitted	**Submit Date:**	8/1/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8382350
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.	The system security rating has been updated from Low to Moderate due to the presence of PII. PII is CDC Username/UserID that is associated with each order that the system processes. Record of all system orders are maintained by the system.
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 purpose of the Core Oder Web Based Ordering System (CoreOrder) is to allow access to an electronic database for inventory and tracking data related to request for oligo and peptide synthesis services, as well as other services for Centers for Disease Control and Prevention (CDC) laboratory research in the Biotechnology Core Facility Branch (BCFB). The system provides a means and allows request/s to be tracked through several stages of the process. The system also provides a laboratorian interface, which allowing full tracking of samples, and assistance in sample management.

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 data stored in the system includes customer full name, user ID, contact information, project information, authorized requester list for the project, and information about each service request such as project number, request date, requester name, Deoxyribonucleic acid (DNA) oligonucleotide types and quantities and product release date.
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 data is collected from the CDC to track and to maintain inventory DNA oligonucleotide types and quantities and product release date.
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.	The purpose of the website is to provide a graphical interface for scientific partners to collaborate on and view scientific data. Only approved CDC personnel are able to authenticate via the website. Approved users are met with a login prompt upon entering the system uniform resource locator (URL) in a browser.
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 User Credentials
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.	51 - 200
PIA - 4:	For what primary purpose is the PII used?	CoreOrder is a web-based ordering system and the primary purpose of using PII is the orders that the system process is placed by CDC users. The PII is CDC Username/UserID that is associated with each order.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Not applicable. The PII (CDC Username, UserID). The PII is only used for order processing and tracking within the system.
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.	The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030; Identity Theft Enforcement and Restitution Act, P.L. 110-326,
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.	PII is non-sensitive business contact information.
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.	The non-sensitive business contact information is required for system operations. Users who do not provide their information will not be able to utilize the system for its intended purpose.
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.	If the system undergoes major changes, individuals will receive an email notice. However, no current process exists to obtain consent.
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 an individual believes their information has been inappropriately obtained, used, disclosed, or the PII is inaccurate, they can contact the point of contact (POC) listed in this document.
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.	This system undergoes triannual recertification as well as annual assessment to review the instances of the non-sensitive business contact information that exist within the system.
PIA - 17:	Identify who will have access to the PII in the system.	Users 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.	Users have access to their own username and email addresses. Administrators have access to the system in its entirety to perform required tasks. Reasons for Users' access to PII (Account number, User ID, Phone Number): Users need access to PII to perform their day-to-day responsibilities. For instance, PII is needed to access and manage accounts, such as update authorized user list of the account. Authorized Users need to the access to place order, check order status and the customer service representatives need the access to assist customers, process orders, deliver products or resolve issues. Reasons for administrators' access to PII (Account number, User ID, Phone Number): Administrators often need access to PII to manage and maintain systems that store or process this data. Their role involves ensuring that the systems are functioning correctly and securely. Setting permissions and access levels for users and ensuring that access to PII is appropriately restricted based on roles and responsibilities. In cases of system issues or data breaches, administrators may need to access PII to identify, troubleshoot, and resolve problems effectively.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The system is configured in such way that users are only permitted when they have authenticated. Administrators configure access controls, ensuring permissions of records are set according to the approved roles and access levels. The projects/accounts expire at the end of each fiscal year. At that time, a renewal process starts to ensure that account details, including user roles and access levels, are updated and accurate.
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.	This system employes role-based access control (RBAC).
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 users are required to participate in annual Cybersecurity Awareness Training and Annual Records Management Training which enforces these practices.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	N/A
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).	The user ID is used for processing and tracking orders within the system. This system adheres to General Record Schedule **(GRS) 5.1** Common Office Records. The disposition instruction for this GRS is to destroy the data when the business use ceases.

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:** Records are maintained according to the CDC's record control schedule and policy. The PII is secured using the CDC/Infrastructure Services (IS) Active Directory authentication process and role-based application control via Role-Based Access Control (RBAC). **Technical:** The network and IT security controls are monitored by the Cybersecurity Program Office (CSPO) and Digital Services Office (DSO). In addition, the image documentation containing PII will be encrypted. **Physical:** Controls are managed by security guards, ID badges, locked doors, and key card restrictions.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	8/2/2024
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:**	8/12/2024
		SOP Days Open:	11

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	8/14/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 8/14/2024 This PIA had comments mainly for the PTA and one minor comment on the PIA. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	On the next iteration of the PTA update the following URL Details: please provide the URL information in th PTA-5A and PTA-5B: Please provide a response as the	**SAOP Review Date:**	8/22/2024
		SAOP Days Open:	8

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	7/29/2024	Selected "user credentials" and deselected other "user id"	
PIA - 7	Data Feed Service, piafrmcdc	7/29/2024	This question must be answered.	
PIA - 18	Data Feed Service, piafrmcdc	7/29/2024	What are the required tasks for administrators?	
PIA - 19	Data Feed Service, piafrmcdc	7/29/2024	Please describe the actual processes and procedures in place.	
PIA - 21	Data Feed Service, piafrmcdc	7/29/2024	Please state the cadence of trainings.	
PIA - 22	Data Feed Service, piafrmcdc	7/29/2024	This answer can be deleted.	
PIA - 23	Data Feed Service, piafrmcdc	7/29/2024	Please cite an actual record control number.	
PIA - 24	Data Feed Service, piafrmcdc	7/29/2024	This answer is insufficient. Please provide these system's specific administrative, physical, and technical controls.	
PIA - 1	VILLAFUERTE, NESTOR	8/13/2024	Does the system have an ATO date? PTA-4 - First instance of "Core Order" is mispelled. PTA-5 - Please Provide a response.	
PIA - 20	VILLAFUERTE, NESTOR	8/13/2024	Please correct spelling of "employs".	
PIA - 1	BLAND, CRYSTAL	8/14/2024	On the next iteration of the PTA update the following: URL Details: please provide the URL information in these fields as they are currently blank. PTA-5A and PTA-5B: Please provide a response as these fields are blank.	

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:	8/22/2024 8:01 PM	**History Log:**	View History Log