








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 - PUBS-WH - QTR3 - 2023 - CDC6829785	PIA ID:	1706986
Name of Component:	CDC - Publication Warehouse System	Name of ATO Boundary:	Publication Warehouse System
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	212
Submission Status:	Re-Submitted	Submit Date:	2/6/2024
Next Assessment Date:	N/A	Expiration Date:	3/7/2027
Office:		OPDIV:	CDC
Security Categorization:	Moderate	OpDiv PIA ID:	CDC6829785
Legacy PIA ID:		Make PIA available to Public?:	No
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.		9/27/2024
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.	The system no longer collects phone number.
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.	CDC-INFO Publication Warehouse System (CDC-INFO PUBSWH) is designed to maintain publication inventory, order fulfillment and all related functions necessary to maintain CDC's Publication Inventory. Data sent to CDC-INFO PUBSWH contains the name and mailing address from the individual who submits the order. Orders can be submitted by anyone (such as general public, businesses, educators, public health professionals).
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.	PUBSWH contains the name and mailing address from the individual who submits the order. CDC-INFO PUBSWH also collects and stores publication identifiers, desired quantity for each publication, and the address where the publication(s) will be shipped. Additionally, CDC-INFO PUBSWH provides CDC with order status and inventory adjustment data.

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 primary purpose of the PII is to fulfill CDC publications orders submitted via the CDC-INFO Pubs website https://wwwn.cdc.gov/pubs (public facing). The data is used to pack and generate shipment info for the fulfillment of orders with its name and mailing address.
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?	
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.	<ol style="list-style-type: none"> 1. Web Ordering (via On Demand - https://wwwn.cdc.gov/pubs/CDCInfoOnDemand.aspx): External Users browse CDC Publications, with the option to download PDF content without providing any PII or order hard copy publications (PII required). 2. Internal Ordering: Each authorized user may only view information associated with specific, assigned administrative codes (admin codes). 3. Information Collected (via On-Demand or PAT) includes Company Name (optional), name, address line 1, address line 2 (optional), city, state, zip, telephone number (For Publication Management use only), email address (optional), and publication(s) ordered. The only POST in the application is the create order call, and the Address Fields are the only PII points. 4. Data Exchange: Publication order data is transmitted to and from the fulfillment warehouse.
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 Mailing Address
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 Patients Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
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?	CDC-INFO Publication Warehouse System (CDC-INFO PUBSWH) is designed to maintain publication inventory, order fulfillment and all related functions necessary to maintain CDC's Publication Inventory. Data sent to CDC-INFO PUBSWH contains the name and mailing address from the individual who submits the order. Orders can be submitted by anyone (such as general public, businesses, educators, public health professionals). The primary purpose of the PII is to fulfill CDC publications orders submitted via the CDC-INFO PUBS website https://wwwn.cdc.gov/pubs (public facing). The data is used to pack and generate shipment info for the fulfillment of orders with its name and mailing address.
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, 42 U.S. Code § 300u.
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.	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	Public Health Service Act, 42 U.S. Code § 300u. Public Health Service Act, 42 U.S. Code § 300u ICR 202301-0920-015 OMB: 0920-1282
PIA - 10B:	Identify the OMB information collection approval number expiration date.	6/30/2026
PIA - 10C:	Explain why an OMB information collection approval number is not required.	Public individuals soliciting feedback and information from Federal Agency, an exemption from Paper Reduction Act and OMB.
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 option to object to the information collection if the individual chooses to order a publication. If the individual does not want to provide PII, he or she will not be able to receive the publication.
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 to notify and obtain consent in the event of a major change to the system. The PII is collected during the ordering process and is only used to fulfill that particular order. There are no situations or major changes anticipated where the PII would be used for anything other than this purpose.
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.	CDC Personnel and the general public, orders the documents through http://wwwn.cdc.gov/pubs/CDCInfoOnDemand.aspx . The CDC-INFO Team may also be contacted via web form at https://wwwn.cdc.gov/pubs/CDCInfoOnDemand.aspx . Or, the individual users may report all concerns about any suspicious activity, disclosure of group email, and/or phone numbers to the representatives at: In Atlanta: 404-639-4282, 404-639-7258 In Hyattsville: 301-458-4583 In Pittsburg: 412-386-6156
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.	Prior to order fulfillment, the address data is checked for accuracy by running the data through a piece of software which is Coding Accuracy Support System (CASS)-certified. CASS certification is offered to all mailers, service bureaus, and software vendors that would like the USPS (United States Postal Services) to evaluate the quality of their address-matching software and improve the accuracy of their, carrier route, and five-digit coding. This data check ensures that the address data is indeed correct and is complete, current, and accurate. Data is not reviewed again as it is never used post-fulfillment.
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.	<p>Users - Users have access to PII to ensure that orders are confirmed.</p> <p>Administrators - Administrators have access to PII to ensure that users have properly verified address information.</p> <p>Developers - Developers have access to the system database as part of their system maintenance duties.</p> <p>Contractors - Direct contractors require access to perform the following roles of users, administrators and developers.</p>
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	<p>Staff who may access PII must work within one of the designated job roles where access to the PII is necessary in order to fulfill the publications orders. System Administrators use the concept of Least Privileged and Role based Account privileges to access PII. Access to the PII is restricted to those with a strict business need-to-know.</p> <p>Administrators have access to facilitate their administration of the systems containing the PII. Fulfillment workers will have access to the PII due to the nature of their job, processing and fulfilling the orders. Developers need access in order to develop and troubleshoot applications associated with the PUBS-WH system.</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.	<p>PII access is based on the concept of least privilege, meaning that all access to PII is restricted to only those users who have a strict business need for access to the information. This is accomplished through the use of access control lists, which are regularly reviewed to ensure that access is still necessary.</p>
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.	<p>All employees are required to complete Information Security and Privacy Awareness Training at least annually.</p>
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).

This item includes requests for information, publications, photographs, and other information involving no administrative action, policy decision, or special compilations or research. The disposition authority (GRS 5.2, Transitory and Intermediary Records Revision - DAA-GRS-2022-0009) indicates They are required for only a short time (generally less than 180 days) and they are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. For specific examples, see the GRS 5.2 Frequently Asked Questions (FAQs).

Exclusion: This item does not include the following data output files, which must be scheduled on an agency-specific schedule: files created specifically for public access purposes, summarized information from unscheduled electronic records or inaccessible permanent records, data extracts produced by a process that significantly changes the content of the file from the source records' content, effectively creating a new data file.

This system automatically deletes data from its database 90 days after the order is received. No other copies of the PII exist after that time.

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:

Security internally is afforded by access control lists, which ensure that access is restricted to those with a strict business need to know.

Technical:

Network security at the perimeter utilizes firewalls which have been appropriately configured and hardened according to industry best practices.

All data is stored on servers which adhere to appropriate information security policy including but not limited to patch management, vulnerability scanning, and remediation.

Physical:

The data is secured in a secured facility. Access to the building is secured through the use of ID badges, which are issued only to those with the appropriate clearances. The perimeter and all points of entry are covered by cameras which record digitally.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	2/7/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: February 7, 2024	Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	
SOP Comments:	Approved on behalf of Beverly Walker	SOP Review Date:	2/8/2024
		SOP Days Open:	2

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	2/12/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 2/12/2024 PIA has been updated however PTA-8 has "Error" display and CDC will have to include "email" in their response to PTA-5 on the next iteration of the PTA. Other than that this PIA is ready for SAOP review and approval. 12/4/2023 This PIA is being return for updates, please update accordingly (see comment below): This PIA says that no change has been made since the last PIA, however the previous PIA says the system has a website and this one said it doesn't have a website. You will need to work with your Archer Support team to address how to resolve the issue with the PTA. Also make sure that PTA-4, Pta-5, or PTA-6 include in their response what system is providing user credentials.	Agency Privacy Analyst Days Open:	4

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:	PIA has been updated however PTA-8 has "Error" display and CDC will have to include "email" in their response to PTA-5 on the next iteration of the PTA. Other than that this PIA is ready for SAOP review and approval.	SAOP Review Date:	3/7/2024
		SAOP Days Open:	24

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	KORAN, ELIZABETH	11/13/2023	The website (https://wwwn.cdc.gov/pubs/CDCInfoOnDemand.aspx) also collects email addresses from individuals ordering publications. Please update your response accordingly.	
PIA - 9	Data Feed Service, piafrmcdc	1/23/2024	If "Members of the Public" are selected, then you must answer 10a-c differently.	
PIA - 1	BLAND, CRYSTAL	2/12/2024	Update on the next iteration of the PTA: PTA-5: please include "email address," in your response.	

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:	3/7/2024 7:02 PM	History Log:	View History Log
----------------------	------------------	---------------------	----------------------------------