

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 - CPAP - QTR1 - 2024 - CDC7787056	PIA ID:	1782338
Name of Component:	CDC - CDC Public Access Platform	Name of ATO Boundary:	CDC Public Access Platform
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	67
Submission Status:	Re-Submitted	Submit Date:	4/2/2024
Next Assessment Date:	N/A	Expiration Date:	4/12/2027
Office:		OPDIV:	CDC
Security Categorization:	Low	OpDiv PIA ID:	CDC7787056
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.		5/15/2024
5:	Is the system or electronic information collection, agency or contractor operated?		Contractor

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?	Both
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 CDC Public Access Platform (CPAP) is to make publications (e.g. journal articles, posters, flier, video, etc.) that come from work supported by federal funding of CDC related research freely available to the general public and scientific community.
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 maintains and disseminates the original work, defined as any content that is being published - e.g. journal article, poster, flier, video, etc. and any business contact information of the author(s) choosing - e.g. name and email. This information was provided by the author(s) at the original publication time for the purpose of dissemination to the public.
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.	This system shares website statistics with another system for determining publishing related statistics. All data shared is collected into statistical information about access for each document published in CPAP. This does not include any sensitive information about individuals.
PTA - 7:	Does the system collect, maintain, use or share PII?	
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)?	Yes
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 CDC Public Access Platform (CPAP) website is to make publications (e.g. journal articles, posters, flier, video, etc.) that come from work supported by federal funding of CDC related research freely available to the general public and scientific community. The public is able to reach the website anonymously.
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?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Does Not 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 Devices Identifiers
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.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	Name/Email is being actively distributed by the author for the purpose of validity, respect, kudos, and citation requirements as it relates to publishing. In some cases, the author may include their OrchID (a disambiguation identifier for authors used by trade journals) so that credit/citation data is accurate.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	User credentials (UserID and Device Identifiers) for server administrators are used to support the administrative login and support activities required to maintain any computer system.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	45 CFR 74.36 (Government Use License) 5 USC 301, Departmental regulations (UserID and DeviceID)
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.	Searches by Author name or email is supported for end users.
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.	None exists. None in development.

PIA - 9:	Identify the sources of PII in the system.	<p>Directly from an individual about whom the information pertains</p> <p>Online</p> <p>Government Sources</p> <p>Within the OPDIV</p> <p>Other Federal Entities</p>
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.	Publication of scientific articles and other media has never required collection approvals. This would be equivalent to requiring a library to keep a collection approval for all of the authors of books in their collection.
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.	<p>For authors, no known civil or criminal penalties are known to exist.</p> <p>For system administrators, it would be considered fraud to fake an in-person proofing or background check.</p>
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.	<p>No opt-out exists.</p> <p>Authors include the data themselves for the purpose of publication. Thus an opt-out is not applicable due to the actions of the author and the de facto requirements of publication. Authors may use a nom de plume or to simply not claim any credit on a published work. The authors imply that they wish their name (and sometimes email) to be collected when they submit their work for publication and include their name/email in the published work.</p> <p>System administrators must be issued UserID and Device ID in order to be an administrator. They may opt to take another job if they do not wish to have a userid or device ID issued to them.</p>

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. The current model of disclosure related to publications is a fundamental objective of the system and there is no expectation that this will ever change.
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.	CPAP has a help desk (publishinghd@cdc.gov) that is available if there are any concerns. The Office of Science would then be able to address or correct any issues. The corrections would be limited to information as published on the CPAP website.
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.	CPAP does not have the means to review all publications against some master list of worldwide names/emails. Publications go through a clearance process prior to publication and all reviews are done at that time. Once published, the publication is not subject to further editing. A follow-up republication may be done by authors to publish corrections; however, the originals still exist in the system but are marked as superseded with links to the updated publication.
PIA - 17:	Identify who will have access to the PII in the system.	<ul style="list-style-type: none"> Users Administrators Developers Contractors Others
PIA - 17A:	Select the type of contractor.	<ul style="list-style-type: none"> Grantees HHS/OpDiv Direct Contractors Third-Party Contractor (Contractors other than HHS 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: Since the publication is freely available to all persons world-wide, users have access to the published names and email addresses.

Developers: Since the publication is freely available to all persons world-wide, developers have access to the published names and email addresses.

Developers have access to device identifier related PII. This is in order to support the proper rights and access control model used to secure the system.

Contractors: Since the publication is freely available to all persons world-wide, contractors have access to the published names and email addresses. Many contractors serve as system administrators or developers. Contractors have access to device identifier related PII. This is in order to support the proper rights and access control model used to secure the system.

Administrators: Since the publication is freely available to all persons world-wide, administrators have access to the published names and email addresses. Administrators have access to device identifier related PII. This is in order to support the proper rights and access control model used to secure the system.

PIA - 19:

Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

The purpose of the CDC Public Access Platform (CPAP) is to make publications (e.g. journal articles, posters, flier, video, etc.) that come from work supported by federal funding freely available to the general public and scientific community.

The system follows a model of least privilege. As such the following is in effect:

Everyone worldwide will have read access to the author's published name, published work, and published email. This is the primary function of the system and as such does not require specific procedures.

Content administrators (eg Librarians) will have access to add new content for publication. As such, they have write access to publications and the associated meta-data.

Only system administrators have full access and will have access to other system administrator userid and device identifiers.

The process and procedures for granting access to content and system administrators is done handled during on-boarding and out-processing of employees. Access is granted by the business steward.

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.	CPAP is a digital archive of publications (e.g. journal articles, posters, flier, video, etc.) that come from work supported by federal funding from CDC that is freely available to the general public and scientific community. The system follows a model of least privilege. The system only has the minimum necessary access to support publication efforts and administrative access. The administrative individuals are identified during employee on-boarding and are removed during out-processing.
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 take Security and Privacy Awareness Training at least annually.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	System administrators attend a yearly security awareness training and do not receive additional training. Content administrators are allowed to attend an online and in-person training to familiarize themselves with the content management interface.
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).	<p>N/A</p> <p>Publications are kept indefinitely; however, CPAP is not the originator of these materials and would not be subject to a record retention schedule.</p> <p>Administrative userids and deviceids are kept for as long as those persons are employees and are kept in accordance with CDC policy.</p>

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.

Publications, and any PII in the publication:
Note: the full publication is public information and are freely given to all visitors.
Administrative controls cover who should be granted access to update publication data.

Technical controls utilize access control to limit the unauthorized modification of publications and audit modification activities.

Physical controls are provided by Amazon Web services. The controls include physical access limitations, physical security guards, limited access areas. All of this is documented and audited under the FedRAMP authorization framework to meet or exceed NIST SP800-53 physical access controls.

UserID/DeviceID:
Administrative controls include the on-boarding and out-processing procedures in relation to employees and the required annual Security Awareness Training.

Technical controls for UserIDs and DeviceIDs are provided by Microsoft.

Physical controls are supplied by Amazon Web services. The controls include physical access limitations, physical security guards, limited access areas. All of this is documented and audited under the FedRAMP authorization framework to meet or exceed NIST SP800-53 physical access controls.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	4/3/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios	Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	
SOP Comments:	Approved on behalf of Beverly Walker	SOP Review Date:	4/8/2024
		SOP Days Open:	6

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	4/9/2024
Agency Privacy Analyst Review Comments:	Reviewer: Jim Laskowski PTA-5A and PTA-7 didn't sync properly, exported PIA with responses are attached in Supporting Documentation. This PIA is ready for SAOP review and approval.	Agency Privacy Analyst Days Open:	1

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:	PTA-5A and PTA-7 didn't sync properly, exported PIA with responses are attached in Supporting Documentation. This PIA is ready for SAOP review and approval.	SAOP Review Date:	4/12/2024
		SAOP Days Open:	3

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
CPAP PIA_bl.rtf	217570	.rtf	4/9/2024 10:53 AM	0

Comments				
Question Name	Submitter	Date	Comment	Attachment
PIA - 12A	Data Feed Service, piafrmcdc	3/19/2024	Please mark the previous question as voluntary if you cannot provide the legal requirement that mandates the processing of PII.	
PIA - 18	Data Feed Service, piafrmcdc	3/19/2024	please specify the purpose for each type of access listed.	
PIA - 24	Data Feed Service, piafrmcdc	3/19/2024	What are the physical controls?	
PIA - 8	Data Feed Service, piafrmcdc	3/19/2024	The response should be "No" because the system does not contain records about the authors, but rather is used to retrieve federally funded works by that author	
PIA - 18	Data Feed Service, piafrmcdc	3/25/2024	<p>Please list each group as done below with a different purpose (unless the contractor has the same use it can be repeated).</p> <ul style="list-style-type: none"> • Users • Administrators • Developers • Contractors • Others 	
PIA - 1	LASKOWSKI, JAMES	4/9/2024	Please respond to PTA 5-A. The reviewer notes that PTA -7 did not sync.	

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:	4/12/2024 4:01 PM	History Log:	View History Log