Privacy Impact Assessment (PIA): CDC - CDC ILLiad - QTR2 - 2024 - CDC8119686

Created Date: 4/29/2024 4:01 PM Last Updated: 9/30/2024 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 - CDC ILLiad - QTR2 - 2024 - CDC8119686	**PIA ID:**	1816831
Name of Component:	CDC - CDC ILLiad	**Name of ATO Boundary:**	CDC ILLiad
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	56
Submission Status:	Submitted	**Submit Date:**	4/26/2024
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:		**OpDiv PIA ID:**	CDC8119686
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.	5/29/2024
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.	CDC Illiad is an information system used to manage and control document delivery and interlibrary loan requests made by CDC personnel. These requests are processed by the Stephen B. Thacker CDC Library.
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 ILLiad/DocExpress system contains the following personally identifiable information: full name, CDC user ID, phone number, email address, employee status (full time employee or contractor), and mailing address (usually the materials are sent to the CDC campus address). Users access the system using Active Directory. As stated above User Ids are stored in the system. Active Directory is a separate system covered by a separate 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 ILLiad/DocExpress system contains the following personally identifiable information: full name, CDC user ID, phone number, email address, employee status (full time employee or contractor), and mailing address (usually the materials are sent to the CDC campus address). The system also contains data about the books and media with return dates requested by CDC users for loan purposes. Contact information for users of the system is used for the delivery of articles and books to the requesting individuals. Most articles are delivered electronically, and some books are mailed to the campus mailing address. Notifications of the book's status is sent to email addresses.
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 ILLiad Connection Manager – Is used to automatically send and receive information between the ILLiad server and the OCLC systems in routing and managing interlibrary loan requests. This component uses port 443, outbound, to connect with webservices.oclc.org. The ILLiad System Manager – Is used to send emails generated by the staff clients during normal processing. These emails are routed to the CDC smtp server to be sent out. The System Manager also includes an electronic delivery cleanup function which automatically deletes PDF files delivered to users via the ILLiad webserver after 30 days, and each day cleans up Odyssey processing files located on the server. The ILLiad client package includes the ILLiad desktop client used by library staff, the ILLiad Customization Manager used by the library systems team to manage the system configuration, and the ILLiad Staff Manager used to manage the access rights for staff users of the clients. Separate permissions are needed to access each component; only members of the library systems team have access to the Customization Manager and Staff Manager.
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 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.	Above 2000

PIA - 4:	For what primary purpose is the PII used?	Contact information for users of the system is used for the delivery of articles and books to the requesting individuals. Most articles are delivered electronically, and some books are mailed to the campus mailing address. Notifications of the book's status is sent to email addresses.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The PII may be used for reporting purposes to better understand how CDC users are utilizing the system.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable, Social Security Number (SSN) is not collected.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable, Social Security Number (SSN) is not collected.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 USC 301, Departmental regulations, Plain Writing Act of 2010
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 In-person Email Online 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.	Under the Paperwork Reduction Act (PRA), “the public” includes individuals, partnerships, corporations, universities, nonprofit organizations, State, local, and tribal governments and agencies, and other associations and organizations, whether foreign or domestic. Federal agencies are not included in the definition of the public. OMB clearance is not required to collect information from other Federal agencies unless the information will be used for general statistical purposes.
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 formal process in place for opting out. The PII is only activated, if users voluntarily make a request for a book or article through 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.	If there is any major changes, users will be notified via email (using their email on file). There is no formal process for obtaining consent, as users provide their information voluntarily.
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 that believe their PII has been inappropriately obtained, used, or disclosed can contact contact the DocExpress Team office at 404 639-2772 or via email at desupport@cdc.gov. The system owner will work to resolve these types of concerns.
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.	Periodic purges of data are done for users that are no longer eligible for ILL/Document Delivery services (i.e. after they leave the CDC), as well as for users with no recent requests remaining in the system. Updates are made regularly to ensure the data is up to date.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators 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.	User: Individual CDC users can see their own business contact information when logged in to the web interface. They do not have access to anyone else's information by this means. Administrators: Library staff that process requests for articles and books to be delivered to the users access PII. Library staff generating reports about system usage access PII. Library staff administrators have access to the PII for investigatory, reporting, or troubleshooting purposes. Contractors: Direct contractors (using CDC credentials) access the system for managing loan requests and for troubleshooting purposes.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role-based access is utilized. Only library staff involved in processing and delivering interlibrary loan and document delivery requests have access to PII. No CDC personnel outside the library, except for selected Digital Services Office (DSO) technicians, are provided access to the ILLiad/DocExpress system or its database. They are provided access based on their job roles.
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.	Database only contains the minimum amount of information necessary for library staff to perform their jobs. The system does not collect any more information than what is necessary which is business contact information.
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 (including direct contractors) are required to take the annual Security and Privacy Awareness Training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	None.
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).	Scientific and Research Project Records Control Schedule: NCI-1-90-82-4 , Item 4: Research Support, Master file, system, or database created for short-term or routine purposes. Authorized Disposition: if administrative usefulness has been met, the PII is disposed after 5 years or after retirement of the system, depending upon program need for scientific, legal, or business reference. Generally, the most recent 5-7 years worth of request data is kept in the database. User records with no requests within that time period are periodically deleted from the database.
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 include a system security plan, contingency plan, regular back up of files and storage of backups off site, role-based security awareness training, least privilege access enforced through Active Directory groups, separate user and privileged accounts for administrators, policies and procedures in place for retention and destruction of PII, and a corporate incident response team and incident response plans. Technical: Role-based access is utilized to only allow selected administrators the ability to view user PII. Library staff users have access to the information by means of the ILLiad desktop clients, which are only installed on the CDC-issued laptops of library staff. Only those who need such access to perform their job duties have the software installed. Physical: Access is subject to badge/key access to the building, locked doors, and 24/7 security guards.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	4/29/2024
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:**	5/13/2024
		SOP Days Open:	17

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/17/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 5/17/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	4

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	6/3/2024
		SAOP Days Open:	17

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	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 4:01 PM	**History Log:**	View History Log