

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 - PHLIP - QTR2 - 2024 - CDC8270761	PIA ID:	1828449
Name of Component:	CDC - Public Health Law Investigation Platform	Name of ATO Boundary:	Public Health Law Investigation Platform
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	37
Submission Status:	Re-Submitted	Submit Date:	6/5/2024
Next Assessment Date:	N/A	Expiration Date:	6/20/2027
Office:		OPDIV:	CDC
Security Categorization:	Low	OpDiv PIA ID:	CDC8270761
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.		4/30/2024
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.	
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Public Health Law Investigation Platform (PHLIP) currently is used by CDC employees and affiliates, but because federally-funded capacity-building initiatives are currently aimed at supporting public health practitioners around the country in conducting legal epidemiology, there is a pressing need for staff in state, tribal, local, and territorial health departments to use PHLIP to read, analyze, and compare data. For this reason, this change intends to make PHLIP available to public health practitioners who secure SAMS credentials, but use the PHLIP outside the CDC network.
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.	<p>Public Health Law Investigation Platform (PHLIP) will allow staff to capture and analyze public health legal text for research questions. PHLIP will allow multiple users to easily and accurately record, synthesize, and validate this information. This will lead to tremendous time savings. In addition, PHLIP helps to achieve CDC's mission by understanding how to achieve better health outcomes through changes in policy and the law.</p> <p>PHLIP is a data visualization tool that shows information on analyzed public health law data sets.</p>
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.	<p>PHLIP contains information on publicly accessible laws and regulations. Data collected in PHLIP includes: 1) text and citations of laws and policies, 2) interpretations of text by project staff and 3) validation of these interpretations.</p> <p>The information contains snippets of text of public law, identification of which state or jurisdiction that law applies to, and answers to legal epi questions.</p> <p>Email addresses are used to determine unique users in the PHLIP when they log in via basic authentication (username/password) and Personal Identity Verification (PIV) authentication via Secure Access Management System (SAMS). Access will be controlled via the Azure Active Directory (AD). Public Health Law Investigation Platform does have to store the user's corresponding CDC email address and it's stored permanently unless edited by an administrator.</p>
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.	<p>PHLIP contains information on publicly accessible laws and regulations. Data collected in PHLIP includes: 1) text and citations of laws and policies, 2) interpretations of text by project staff and 3) validation of these interpretations. Public Health Law Investigation Platform does have to store the user's corresponding CDC email address and it's stored permanently unless edited by an administrator.</p> <p>The information contains snippets of text of public law, identification of which state or jurisdiction that law applies to, and answers to legal epi questions (e.g. does this jurisdiction have a vaccine requirement for Hep A , yes/no).</p> <p>Email addresses are used to determine unique users in the PHLIP when they log in via basic authentication (username/password) and Personal Identity Verification (PIV) authentication via Secure Access Management System (SAMS). Access will be controlled via the Azure Active Directory (AD). Public Health Law Investigation Platform does have to store the user's corresponding CDC email address and it's stored permanently unless edited by an administrator.</p>
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)?	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.	<p>The purpose of the PHLIP website is to allow CDC staff to capture and analyze public health legal text for research questions. The system will allow staff to create a list of questions for a topic area. The Legal team answers these questions and cites publicly available legal documentation. The Public Health Law Program will use this information to create reports for CDC programs. Additionally, the purpose of the website is allow staff in state, tribal, local, and territorial health departments to use PHLIP to read, analyze, and compare data in order to support public health practitioners around the country in conducting legal epidemiology, since there is a pressing need for staff in state, tribal, local, and territorial health departments to use PHLIP to read, analyze, and compare data.</p> <p>External users will authenticate through Secure Access Management System (SAMS) and be granted direct access to PHLIP. Their access will be controlled via the Azure Active Directory (AD). Public Health Law Investigation Platform does have to store the user's corresponding CDC email address and it's stored permanently unless edited by an administrator.</p>
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.	Other Other technology - 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
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.	51 - 200

PIA - 4:	For what primary purpose is the PII used?	Names are used to track who entered information.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	Email addresses are used to determine unique users in PHLIP when they log in via basic authentication (username/password) and PIV authentication via SAMS.
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.	N/A
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 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.	N/A -PHLIP does not collect information directly from the public. Rather the user uses SAMS (username/password) to access PHLIP.
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.	Individuals are required to consent to PII for business practices. If an individual requests to opt out, they are unable to fulfill required job duties.

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.	The Public Health Law Investigation Platform (PHLIP) administrator will notify and obtain consent of individuals whose PII is in when major change occur via email.
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.	For concerns pertaining to PII individuals can contact the PHLIP Security Team at PHICITSecurityTeam@cdc.gov.
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.	A yearly review regarding the PII elements is performed by the Business, Technical, and Security Stewards in which the PIA is reviewed and submitted to the Chief Privacy Officer of the CDC. Additionally, the Business, Technical, and Security Stewards, as well as the Program and Project Managers, also participate in regular briefings that include information on upcoming system changes or when major changes occur.
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 - Users in PHLIP do not have access to projects beyond their own, therefore they would not have access to the PII for others within the system. Administrators - Administrators assign use permissions to access PHLIP, therefore access to PII is required.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role Based Access Control (RBAC) procedures are in place and assigned via management to ensure that only authorized users and administrators are able to access information. User must be an administrator to have right to view e-mail addresses.
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.	Least Privilege is used and assigned via management to ensure that administrators access only the information needed to complete job functions. When a user requests access to the PHLIP, the program determines the need for access, and if access is granted the individual is advised that they will access PHLIP using their user id and other pertinent information to complete the identity, authentication, and access process.

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.	Personnel will undergo yearly privacy and security awareness training that outlines their responsibility for protecting information being collected and maintained. In addition, personnel must assert their understanding CDC Implementation of the HHS Rules of Behavior (For Use of HHS Information Technology Resources) which reinforces the responsibility of protecting the information being collected and maintained.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Role Based Training required for any Privileged Users. Users will have access to a user guide as well as in-person training from the PHLIP administrator.
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).	Destroy 2 years after standard is superseded, canceled, or disapproved by The Office of Personnel Management OPM (as appropriate) but longer retention is authorized if required for business use. DAA-GRS-2014-0002-000.1
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.	<p>PII will be secured through the use of the following controls:</p> <p>Administrative: Least Privilege and Role Based Access methodologies are in place. Additionally, mandatory security and privacy awareness training is required for all users; including role-base training for any user with administrative privileges.</p> <p>Technical: Role-based access controls are being used based upon the role of the individual and based upon administrative privileges. Federal Information Standards (FIPS) 140-2 for encryption will be used for transmission and data at rest. Non-repudiation is achieved through the support of digital signatures and encrypted email using PIV.</p> <p>Physical: Controlled physical access within data centers, monitored access to components, emergency shutoff systems, and fire and water damage protections are in place.</p>

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	6/6/2024
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:	6/10/2024
		SOP Days Open:	5

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	6/11/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 6/11/2024 The comments made in reference to the PTA are minor and can be updated on the Next iteration of the PTA. This PIA is ready for SAOP review and approval. PIA-1 - If "Name" is one of the PII elements collected, please include it in your response in PTA-5 and PTA-6. PTA-2 - Reviewer notes that this section failed to sync. Confirm the response for PTA-2 is "New Public Access." See Supporting Documentation. PTA-2A - Please spell out acronym "SAMS" in its first instance (It is spelled out in PTA-5). PTA-9 - Please include the publicly accessible website's URL (Reviewer is unable to see the URL detail subpage).	Agency Privacy Analyst Days Open:	1

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:	he comments made in reference to the PTA are minor and can be updated on the Next iteration of the PTA. This PIA is ready for SAOP review and approval. PIA-1 - If "Name" is one of the PII elements collected, please include it in your response in PTA-5 and PTA-6. PTA-2 - Reviewer notes that this section failed to sync. Confirm the response for PTA-2 is "New Public Access." See Supporting Documentation. PTA-2A - Please spell out acronym "SAMS" in its first instance (It is spelled out in PTA-5). PTA-9 - Please include the publicly accessible website's URL (Reviewer is unable to see the URL detail subpage).	SAOP Review Date:	6/20/2024
		SAOP Days Open:	9

Supporting Document(s)				
Name	Size	Type	Upload Date	Downloads
CDC_PHILP_PIA_bl (7).rtf	210497	.rtf	6/11/2024 12:20 PM	0

Comments				
Question Name	Submitter	Date	Comment	Attachment
PIA - 15	Data Feed Service, piafrmcdc	5/15/2024	Please remove PII and put an organizational email address or phone number.	
PIA - 24	Data Feed Service, piafrmcdc	6/4/2024	Please use complete sentences.	
PIA - 1	VILLAFUERTE, NESTOR	6/10/2024	<p>PIA-1 - If "Name" is one of the PII elements collected, please include it in your response in PTA-5 and PTA-6.</p> <p>PTA-2 - Reviewer notes that this section failed to sync.</p> <p>PTA-2A - Please spell out acronym "SAMS" in its first instance.</p> <p>PTA-9 - Please include the publicly accessible website's URL.</p>	

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:	6/20/2024 8:01 PM
History Log:	View History Log