

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 - NCHHSTP IP - QTR1 - 2024 - CDC8003102	PIA ID:	2552239
Name of Component:	CDC - NCHHSTP Informatics Platform	Name of ATO Boundary:	NCHHSTP Informatics Platform
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	316
Submission Status:	Submitted	Submit Date:	12/18/2024
Next Assessment Date:	N/A	Expiration Date:	1/15/2028
Office:		OPDIV:	CDC
Security Categorization:		OpDiv PIA ID:	CDC8003102
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.	No changes
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.	NCHHSTP-Informatics Platform (NCHHSTP-IP) system was developed to support effective and efficient applications access for CDC employees, contractors and participating external users. NCHHSTP-IP acts as a service to authenticate and authorize specific access to multiple applications, both internally and externally facing, for both CDC and these external users.

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.	NCHHSTP IP stores and maintains metadata that is specific to an "application". The metadata includes a user id (user name) business contact information (business title, business address, business phone number and business email), accessible application(s) and access permissions. Internal users authenticate via Active Directory. (AD) is used for access control/authentication of CDC users. AD is covered by a separate PIA. External users authenticate using Secure Access Management System (SAMS). SAMS is 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.	NCHHSTP IP stores and maintains metadata that is specific to an "application". The metadata is subsequently used by participating applications to allow users access to explicit functionality. The metadata includes user id, username, business title, business address, business phone number and business email, accessible application(s) and access permissions. NCHHSTP IP system has a web site for system administrators to perform necessary administrative and management functions including updating authorized applications and authorized users and access permissions. Only authorized CDC employees or contractors are allowed to access the web site to perform necessary administrative and management functions.
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 NCHHSTP IP is to support effective and efficient applications access for CDC employees, contractors and participating external users. NCHHSTP IP Partners and Public Health professionals have access via AD for internal users and SAMS for external users.
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 - 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.	Email Address Phone numbers Mailing Address Other - Free text Field - Username and Title
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.	201 - 500
PIA - 4:	For what primary purpose is the PII used?	The primary purpose for the PII is to enable user access.
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.	Section 306 of the Public Health Service Act (42 USC 242k)
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
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.	Required for system access
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.	When contact is made, users can opt-out of the collection of their business contact, however, information is needed in order to obtain access to NCHHSTP IP systems
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.	NCHHSTP IP does not foresee any changes occurring. However, if major changes occur, impacted individuals would be contacted by either the NCHHSTP IP's Technical, Security, or Business Steward.
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 has concerns that their PII has been inappropriately obtained, used, disclosed or inaccurate, the individual can contact the NCHHSTP IP Business or Technical Steward (as identified in this document) for action.

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 reviews are performed annually. When an individual no longer requires access, the Business Steward will coordinate with the Technical Steward for access, updates and removal.
PIA - 17:	Identify who will have access to the PII in the system.	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.	CDC employees who will have access to assign roles and provide system access.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role-based access controls are implemented at the server level in to ensure only individuals with a need to know have access to the PII.
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 model is utilized based on User ID in conjunction with Active Directory to limit access to files containing PII within the system.
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.	Security and Privacy Awareness Training (SAT) is required annually.
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).	Records are retained and disposed of in accordance with the National Archives and Records Administration (NARA) General Records Schedule 3.2: Information Systems Security Records, which indicate: Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

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.

Administration:

CDC personnel are required to complete the annual OCISO Security Awareness Training to make them aware of their responsibilities for protecting the information being collected and maintained.

Technical:

Access to the server is controlled using individual access controls; username and password, and only authorized users will have access to the data.

Physical:

The servers are housed in a secure CDC computer room that require building and room electronic access using the individuals Personal Identity Verification (PIV) card. The Chamblee campus has a 24/7 gate guard that requires use of the individuals PIV card and a valid parking sticker to gain access.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	12/18/2024
Privacy Analyst Comments:		Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	
SOP Comments:	Approved on behalf of Beverly Walker	SOP Review Date:	1/2/2025
		SOP Days Open:	15

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	1/8/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 1/8/2025 CDC confirm that for PTA-12A that Session cookies does not collect PII (see email in Supporting Documentation). This PIA is ready for SAOP review and approval.	Agency Privacy Analyst Days Open:	6

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:	1/8/2025 CDC confirm that for PTA-12A that Session cookies does not collect PII (see email in Supporting Documentation). This PIA is ready for SAOP review and approval.	SAOP Review Date:	1/15/2025
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
1-8-2025 Re_NCHHSTP IP - QTR1 - 2024 - CDC7950435.pdf	201902	.pdf	1/8/2025 9:55 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 10	Data Feed Service, piafrmcdc	1/2/2025	Ignore	
PIA - 1	BLAND, CRYSTAL	1/7/2025	<p>On the next iteration of the PTA:</p> <p>PTA-5A and PTA-5B: Please provide a response, if applicable.</p> <p>1/8/2025 Per CDC email PTA-12A response should be "Session Cookies - Do Not Collect PII."</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:	1/15/2025 1:02 PM	History Log:	View History Log
---------------	-------------------	--------------	----------------------------------