Privacy Impact Assessment (PIA): CDC - PPRL - QTR3 - 2025 - CDC8733805

Created Date: 8/1/2025 4:00 PM Last Updated: 8/29/2025 8:01 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 - PPRL - QTR3 - 2025 - CDC8733805	**PIA ID:**	3584847
Name of Component:	CDC - Privacy Preserving Record Linkage (PPRL)	**Name of ATO Boundary:**	Privacy Preserving Record Linkage (PPRL)
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	50
Submission Status:	Re-Submitted	**Submit Date:**	8/19/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8733805
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Development
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	
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.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
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.	The Privacy Preserving Records Linkage (PPRL) is a transformative solution for secure Date Linkage in Public Health. PPRL system provides de-identified matching of anonymous patient records to each other creating an anonymous but longitudinal view of patient activity. The system matches submitted de-identified patient information and returns a proprietary identifier so that records pertaining to a single patient can be linked in an anonymous and interoperable manner. PPRL is used to support the HealthVerity system that provides Immunization Information System (IIS) Jurisdictions with an on-premises De-Identification Engine, that allows jurisdictions to securely de-identify patient records within their IISs. The de-identified data is then uploaded to the PPRL system where it is added to a Master Patient List (MPL) database.
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 information collected (into), maintained, and/or shared in the system are: Business Contact Information (BCI) Name, and Email Address provided to HealthVerity is not stored, but temporarily used to create alternative user ID. The data accessed on QuickSight will include, Year, Month, Number of Valid Records, Site Name, Total Records, Number of Zip Code error, Number of New Records, Number Records, this data on PPRL will be saved indefinitely for future use in the application.
PTA - 5A:	Are user credentials used to access the system?	
PTA - 5B:	Please identify the type of user credentials used to access the system.	Non-HHS User Credentials Username Password
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.	Name, and Email Address is provided to HealthVerity to create CDC users an Account Name to access the web application (QuickSight). PPRL captures the following categories as numerical values, Year, Month, Number of Valid Records, Site Name, Total Records, Number of Zip Code error, Number of New Records, Number of Records. This metrics data is used to analyze the quality of data received, then provide feedback to jurisdictions to help improve data quality. A proprietary identifier is also maintained to enable anonymous and interoperable linkage of records pertaining to a single patient.
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)?	
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.	https://us-east-1.quicksight.aws.amazon.com The website holds an operational dashboard hosted within Amazon Web Service (AWS) QuickSight. AWS QuickSight is a Federal Risk and Authorization Management Program (FedRAMP) Moderate authorized service. Centers for Disease Control and Prevention (CDC) users authenticate into the dashboard through Okta. HealthVerity employees authenticate through Okta Security Assertion Markup Language (SAML) via AWS Identity Center Single Sign-On (SSO).
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?	Yes
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 Other - Free text Field - User Id, Passwords
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.	Below 50
PIA - 4:	For what primary purpose is the PII used?	Name and Email is collected and used to create a user account and provide an alternative user ID. The Name and Email address is collected from 3 CDC Employees and used to create a user ID that grants them access to the PPRL Quick sight Dashboard.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	None
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable. Social Security Numbers or Taxpayer ID are not used.
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.	The legal authority governing information use and disclosure specific to the system is Public Health Service Act, section 301.
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.	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.	An OMB is not required as the Name and Email address collected are used to create 3 users alternative IDs. The respondents are CDC employees acting within the scope of their employment. Hence an OMB number collection approval is not required.
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.	The users may elect to decline to participate in the Privacy Preserving Record Linkage (PPRL) project, and their name and email address will not be provided to HealthVerity for user ID creation.
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.	No major system changes related to disclosure are expected through the PPRL, however, if a change is to be affected, the three CDC users will be communicated through 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.	The 3 CDC users may express concerns about their contact information (email and name) by first notifying the CDC PPRL project and then sending an email to Integrations@healthverity.com and express their 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.	No processes are in place for periodic reviews because PPRL has no patient level PII contained in the system for data's integrity, availability, accuracy and relevancy. When a user account is no longer needed, the CDC project team will notify the PPRL administrators to remove the user access from the PPRL System
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators
PIA - 17A:	Select the type of contractor.	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?	

PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	PPRL has no patient level PII contained in the system. Users have access to the dashboard to view de-identified data in a form of numeric values that will Not identify any individuals. Administrators (Healthverity) are provided the Name and Email address for the purposes of creating an alternative user ID that allows CDC users access to the PPRL Quicksight Dashboard and removal of the user account when no longer needed.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access rights are assigned based on predefined roles that align with users' job responsibilities and the principle of least privilege. Users requesting access to the PPRL application would be required to provide documented justification, reviewed and approved by the designated authority. Periodic access reviews are conducted to validate the continued need for each user's access.
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.	The PPRL system is built with controls that include Role-Based Access Control (RBAC): Limits system access to authorized personnel based on job function. Audit Logging and Monitoring**:** Continuous logging of access and modification activities, with real-time alerting for suspicious behaviors.
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.	CDC users complete annual IT security and privacy awareness training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Not Applicable. There is no additional training provided to users
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).	User accounts and associated credential information are removed when no longer needed for access. The user accounts are temporary records and not subject to long term records retention. CDC Records Control Schedule 01-01-01d Office Administrative Files. User accounts are reviewed annually.

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 security plan, contingency plan, and training. Access reports are reviewed daily. Access to PPRL is approved by the program and Health verity. Technical: These include automated safeguards built into the system and its infrastructure: **Encryption:** Data is encrypted at rest and in transit using industry-standard encryption protocols **Multi-Factor Authentication (MFA):** Applied to all user access points to prevent unauthorized logins. **Role-Based Access Control (RBAC):** Limits system access to authorized personnel based on job function. **Audit Logging and Monitoring:** Continuous logging of access and modification activities, with real-time alerting for suspicious behaviors. **Vulnerability Management:** Regular patching and scanning to eliminate security weaknesses that could expose any data within the PPRL system Physical: PPRL is a cloud system, the data center where the system is hosted has the below physical security control: Physical Access is restricted to authorized personnel using security badges, biometric authentication, and surveillance systems. Fire suppression systems, climate control, and disaster recovery mechanisms to prevent data loss from physical threats. Strict protocols for verifying, logging, and escorting visitors to areas where PII is stored.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	8/20/2025
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:**	8/20/2025
		SOP Days Open:	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	8/22/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 8/22/2025 All comments have been addressed this PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	SAOP signature.docx
SAOP Comments:		**SAOP Review Date:**	8/29/2025
		SAOP Days Open:	7

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	8/1/2025	In accordance with the previously approved PTA, there are some data elements that are missing. Please explain why the data elements are not included in the response or please add the data elements to the response. **The PTA states the following:** **The information collected (into),**	

			maintained, and/or shared in the system are: **Business Contact Information (BCI) Name, and Email Address provided to HealthVerity is not stored, but temporarily used to create alternative user ID.** **The data accessed on QuickSight will include, Year, Month, Number of Valid Records, Site Name, Total Records, Number of Zip Code error, Number of New Records, Number Records, this data on PPRL will be saved indefinitely for future use in the application.**
PIA - 4	Data Feed Service, piafrmcdc	8/1/2025	The name, email address, and user id should be added to PIA-2, as they are PII data elements.
PIA - 10C	Data Feed Service, piafrmcdc	8/1/2025	The contact information should be added to PIA-2, as they are PII data elements.
PIA - 24	Data Feed Service, piafrmcdc	8/1/2025	Please refrain from using technical jargon. Let's not give the public information that would make us vulnerable to an attack by providing them an example of the type of encryption that may be used. Please remove, "like AES-256 and TLS 1.2 or higher." The response can be stated as, **"Data is encrypted at rest and in transit using industry-standard encryption protocols."**
PIA - 1	Data Feed Service, piafrmcdc	8/4/2025	In accordance with the previously approved PTA, there are some data elements that are missing. Please explain why **ALL of** the data elements are not included in the response or please **add ALL** of the data elements to the response.
PIA - 1	Data Feed Service, piafrmcdc	8/5/2025	The other Data processed and maintained by the PPRL system such as: Year, Month, Number of Valid Records, Site Name, Total Records, Number of Zip Code error, Date of Birth Error, Number of New Records, Number of Records, File Size, PPRL ID Rate, Valid Records, Invalid/Null records, Patient Name Error, Existing PPRL IDs, New PPRL IDs. are only numeric identifies. The PPRL system does not collect, store or process the underlying information that these

			numeric values are derived from. A screenshot of those numerical data types can be found in the attachment below.	
PIA - 7	Data Feed Service, piafrmcdc	8/18/2025	Legal authority is required.	
PIA - 1	VILLAFUERTE, NESTOR	8/21/2025	Please provide a response to PTA-8a Reviewer notes that PTA-7,and PTA 11a failed to sync. Reviewer notes that the system is missing an ATO date.	
PIA - 1	BLAND, CRYSTAL	8/22/2025	Per CDC's Email and Attachment, the following comments are addressed: **Q4:** Is there a planned ATO date? No **PTA-7:** response did not sync. Does the system collect, maintain, use, or share PII? Yes **PTA-8A:** response is blank. Are any URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications? No **PTA-11**: is marked “Yes” but when you input the URL in it take you to a logon screen and there are no links to non-federal government websites. Should this response be “No?” Yes	8-22-2025 EMAIL_Re_ CDC - PPRL - QTR3 - 2025 - CDC8733805.pdf 8-22-2025 PPRL_PIA.rtf

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:	8/29/2025 8:01 PM	**History Log:**	View History Log