Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-29684 | Form Date: 3/15/2018 9:02:01 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-1557750-345723
2a	Name:	Childhood Blood-Lead Surveillance System (CBLS)
3	The subject of this PIA is which of the following?	○ General Support System (GSS) ○ Major Application ○ Minor Application (stand-alone) ◉ Minor Application (child) ○ Electronic Information Collection ○ Unknown
3a	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
3b	Is this a FISMA-Reportable system?	○ Yes ◉ No
4	Does the system include a Website or online application available to and for the use of the general public?	○ Yes ◉ No
5	Identify the operator.	◉ Agency ○ Contractor
6	Point of Contact (POC):	POC Title: Business Owner POC Name: David Wright POC Organization: NCEH POC Email: ybq2@cdc.gov POC Phone: 770-488-4715
7	Is this a new or existing system?	◉ New ○ Existing
8	Does the system have Security Authorization (SA)?	◉ Yes ○ No
8a	Date of Security Authorization	Sep 19, 2018

Save

11	Describe the purpose of the system.	Childhood Blood-Lead Poisoning Surveillance (CBLS) system is a surveillance and analysis system used to maintain and report
12	Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)	The system maintains laboratory blood lead testing information (child_id, address_id, test result, submission year, submission quarter) for children exposed to lead. Each State collects the information, and CDC receives demographic
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	Lead exposure has been linked to a number of health effects and even relatively low blood lead levels can have a negative and long lasting effect on the cognitive skills, behavior, and
14	Does the system collect, maintain, use or share **PII**?	(•) Yes ( ) No
15	Indicate the type of PII that the system will collect or maintain.	☐ Social Security Number ☒ Date of Birth ☐ Name ☐ Photographic Identifiers ☐ Driver's License Number ☐ Biometric Identifiers ☐ Mother's Maiden Name ☐ Vehicle Identifiers ☐ E-Mail Address ☐ Mailing Address ☐ Phone Numbers ☐ Medical Records Number ☐ Medical Notes ☐ Financial Account Info ☐ Certificates ☐ Legal Documents ☐ Education Records ☐ Device Identifiers ☐ Military Status ☐ Employment Status ☐ Foreign Activities ☐ Passport Number ☐ Taxpayer ID Race City, State, and zip code Gender Ethnicity
16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	☐ Employees ☐ Public Citizens ☐ Business Partners/Contacts (Federal, state, local agencies) ☐ Vendors/Suppliers/Contractors ☒ Patients Other
17	How many individuals' PII is in the system?	1,000,000 or more
18	For what primary purpose is the PII used?	The PII is primarily used for childhood blood lead surveillance and analysis.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	A secondary use for the PII is research and training.
20	Describe the function of the SSN.	N/A

Save

20a	Cite the **legal authority** to use the SSN.	N/A
21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	Public Health Service Act, section 301, "Research and Investigation, " (42 U.S.C. 241); and Sections 304, 306, and 308(d) which discuss authority to maintain data and provide assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)).
22	Are records on the system retrieved by one or more PII data elements?	○ Yes ◉ No
23	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains ☐ In-Person ☐ Hard Copy: Mail/Fax ☐ Email ☐ Online ☐ Other Government Sources ☐ Within the OPDIV ☐ Other HHS OPDIV ☒ State/Local/Tribal ☐ Foreign ☐ Other Federal Entities ☐ Other Non-Government Sources ☐ Members of the Public ☐ Commercial Data Broker ☐ Public Media/Internet ☐ Private Sector ☐ Other
23a	Identify the OMB information collection approval number and expiration date.	
24	Is the PII shared with other organizations?	○ Yes ◉ No
25	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.	There is no prior notice given by CDC because CDC does not collect the data directly from the individuals. Data is collected and submitted to CDC by State and Local public health agencies.
26	Is the submission of PII by individuals voluntary or mandatory?	◉ Voluntary ○ Mandatory
27	Describe the method for individuals to 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 have no means of opt-out. in most jurisdictions where CBLS data is initially collected all blood lead test laboratory records must be reported to the state or local public health authority. States remove major identifying information from patient records and submit to CDC for aggregation, analysis and reporting.

Save

28	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.	CDC does not have a process to notify and obtain consent from individuals in the event of a significant system change. The reason for this is that CDC is not provided names nor any contact information by the state/local public health authorities.
29	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.	It is not necessary to implement this process since the de-identified data released or reported by CDC is not unique to the individual but is only reported in aggregates. CDC is not provided names nor any contact information by the state/local public health authorities; all data is collected and submitted to CDC by State and Local public health agencies.
30	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.	CBLS does not contain PII in the system. All child blood lead data is de-identified from state and local agencies prior to submission to CDC. CBLS data is cleansed quarterly for data integrity, accuracy and relevancy. The data is reviewed for accuracy, file duplication and all fields are reviewed for relevancy and consistency. This file is provided to the data manager for validation. The Data Manager transfers the data via secure FTP to an encrypted shared drive for validation & processing into the encrypted CBLS database. If changes or updates to the data files are required those changes are completed based on the validation process. The cleaned and validated file is now the official file.
31	Identify who will have access to the PII in the system and the reason why they require access.	☐ Users ☒ Administrators: Full access for data management and maintenance ☐ Developers ☐ Contractors ☐ Others
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Per a role-based access model, access to PII in the Childhood Blood Lead Surveillance (CBLS) system is determined by the Business Steward. Administrators, Data Managers, and Project
33	Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	The least privilege model is applied to access PII. Least privilege provides the user with only those privileges which are essential to perform their intended job function. Managers can only access PII after having the managerial group permission associated to their account by the system Business Steward. Examples of controls that are employed are: Read/Write permissions that are controlled by user roles and privileges; Windows authentication; and Active Directory controls for administrative access and audit logs.

Save

34	Identify training and awareness provided to personnel (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 system administrators must undergo annual Security and Privacy Awareness training (SAT).
35	Describe training system users receive (above and beyond general security and privacy awareness training).	All system administrators have extensive training and experience maintaining database management systems and best practices related to public health surveillance and reporting systems.
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	(•) Yes ( ) No
37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Records are retained and disposed of in accordance with the CDC Records Control Schedule B321 and B371. Record copy of study reports are maintained in agency from two to three years in accordance with retention schedules. Source documents for computer are disposed of when no longer needed by program officials. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. Records are retained for 20 years; for longer periods if further study is needed.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative: The HHS Rules of Behavior govern the data protection, integrity and general use of the system and data rights. Only users with proper role based access privileges (Centers for Disease Control / National Centers for Environmental Health / Lead Poisoning Prevention Branch (CDC/NCEH/LPPB) staff have Active Directory (AD) rights to access the network and only approved individuals (Data manager, data stewards, and system users) have privileges to access data directly. CDC approved credentials are used to access the system, based on the principles of least privilege Technical: Active Directory, Windows Authentication, Audit Logs Physical: Production and test servers are stored in a server room secured by the CDC. Access tools are in place to secure entry into CDC buildings (Guards, ID Badges, Key Card, and Closed Circuit TV).
General Comments		
OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S	Digitally signed by Beverly E. Walker -S Date: 2018.09.19 14:59:13 -04'00'

Save