Save

Privacy Impact Assessment Form

v 1.45

Status: Draft | Form Number: F-20292 | Form Date: 1/27/2015 7:25:07 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-3096596-687484
2a	Name:	Laboratory Based Enteric Disease Surveillance (LEDS)
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 Steward POC Name: Patti Griffin POC Organization: CDC/OID/NCEZID POC Email: pmg1@cdc.gov POC Phone: 404.639.3384
7	Is this a new or existing system?	◉ New ○ Existing
8	Does the system have Security Authorization (SA)?	○ Yes ◉ No
8b	Planned Date of Security Authorization	February 19, 2015 ☐ Not Applicable

Save

11	Describe the purpose of the system.	LEDS is a combination of CDC-developed message handlers and SAS programs that capture, store and analyze laboratory confirmed isolate information obtained through the transmittal and receiving of isolate information from external laboratories. Data from this system is used by CDC for disease surveillance and analysis. There are four programs that participate and receive some or all of their data via this system: Foodborne, Influenza, Rabies and FoodNet.

Save

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.)	Four independent programs fall under the umbrella that is called LEDS. Each program collects the same basic demographic information and differentiates themselves by the additional information each collects. The external sites are provided detailed instructions on how to create the disease specific ASCII delimited files from their Laboratory Information Management System (LIMS). They send these files via CDC's Public Health Information Network Messaging System (PHINMS). The information collection and analysis requirements of the LEDS programs are managed independently through their corresponding CDC divisions as follows: Division of Foodborne, Waterborne and Environmental Diseases (NCEZID\DFWED) • Foodborne o Diseases: Campylobacteriosis, Escherichia coli, Salmonellosis, Shigellosis o Detailed isolate information is collected along with minimal demographic information such as State, Zip code, County, Sex, Ethnicity, Race and Age. • FoodNet o Diseases: Campylobacteriosis, Cholera, Cryptosporidiosis, Cyclosporiasis, Escherichia coli, HUS, Listeriosis, Salmonellosis, Shigellosis, Yersiniosis o Detailed isolate information is collected along with minimal demographic information such as State, Zip code, County, Sex, Ethnicity, Race and Age. Once or twice a year, case studies are conducted and the interview questions are transmitted and added to the database. No PII data is collected for case studies. Influenza Division (NCIRD/ID) • Influenza o Diseases: Influenza o Detailed isolate information is collected along with minimal demographic information such as State, Zip code, County, Sex, Ethnicity, Race and Age. Division of High-Consequence Pathogens and Pathology (NCEZID\DHCPP) • Rabies o Diseases: Rabies o Detailed isolate information is collected along with minimal demographic information such as State, Zip code, County, Sex, Ethnicity, Race and Age.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	LEDS is a combination of CDC-developed message handlers and SAS programs that capture, store and analyze laboratory confirmed isolate information obtained through the transmittal and receiving of isolate information from external laboratories. Data from this system is used by CDC for disease surveillance and analysis. There are four programs that participate and receive some or all of their data via this system: Foodborne, Influenza, Rabies and FoodNet. Detailed isolate information is collected along with minimal demographic information such as State, Zip code, County, Sex, Ethnicity, Race and Age.
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 Ethnicity Race County Gender Zip code
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 used by programs for disease surveillance and statistical analysis.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	n/a
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 306(b) (42 U.S.C. 242k)
22	Are records on the system retrieved by one or more PII data elements?	○ Yes ◉ No
22a	Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.	Published: Published: Published: ☐ In Progress
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.	Not-Applicable
24	Is the PII shared with other organizations?	○ Yes ◉ No
24a	Identify with whom the PII is shared or disclosed and for what purpose.	☐ Within HHS ☐ Other Federal Agency/Agencies ☐ State or Local Agency/Agencies ☐ Private Sector

Save

24b	Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
24c	Describe the procedures for accounting for disclosures	
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.	No prior notice is given. All information is obtained at the State Health Department level. CDC does not interact with any individual and therefore all responsibility for patient notification resides with the State.
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.	No option exists. All information is obtained at the State Health Department level. CDC does not interact with any individual and therefore all responsibility for patient notification resides with the State. The LEDS system receives data after patient has voluntarily shared Data with the state Department of Health with the express knowledge that such data may be shared with other relevant entities/organizations.
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.	State health department has the notification responsibilities as they are the collectors and originators of the data. Changes are received into LEDS System secondarily.
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.	The Security Steward and Information System Security Officer (ISSO) are notified and analyze the incident. If the incident proves that PII was disclosed, CSIRT and the CPO are notified within one hour. At CDC's direction, the corresponding State health departments will be engaged to notify affected individuals since they are the collectors/originators of the data.
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.	OCISO requires annual security control assessment of the systems confidentiality, integrity, and availability. In addition, data cleaning and error reporting routines run on every State Health Laboratory record received to ensure the data's accuracy and relevance. At the end of each calendar year, final reviews and corrections (if necessary) are conducted before the calendar year data file is finally “Closed Out” and made available for analysis and publication by the program in papers and journals.

Save

31	Identify who will have access to the PII in the system and the reason why they require access.	☐ Users	
		☒ Administrators	Full Access to properly manage data
		☒ Developers	Read/Write Access in order to help maintain data and its accuracy
		☐ Contractors	
		☒ Others	SME; Read Access Level to help interpret meaning of data
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role-based Access Control (RBAC)	
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 used	
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.	Annual CDC Security and Privacy Awareness Training (SAT)	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Role-based Training to use the database is given to individuals with access priviledges.	
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.	Final reports and substantive reporting materials are maintained permanently (CDC RCS, B-321, 4). Other input/ output records and system data that may be required for follow-up are disposed of after 10 years. 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. In addition, electronic media is subject to ITSO zero-wipe pass methodology.	
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Operational Controls include physical facilities management policies, data center and media protection procedures, security & privacy incident response procedures; and mandatory annual security & privacy awareness training; and Technical Controls include application level role based access controls; servers audit and accountability requirements; encryption of PII at rest and in transit; and adherence to organizationally defined minimum security controls.	

REVIEWER QUESTIONS: The following section contains Reviewer Questions which are not to be filled out unless the user is an OPDIV Senior Officer for Privacy.

Reviewer Questions	Answer

Save

	Reviewer Questions	Answer
1	Are the questions on the PIA answered correctly, accurately, and completely?	◯ Yes ◯ No
Reviewer Notes		
2	Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	◯ Yes ◯ No
Reviewer Notes		
3	Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	◯ Yes ◯ No
Reviewer Notes		
4	Does the PIA appropriately describe the PII quality and integrity of the data?	◯ Yes ◯ No
Reviewer Notes		
5	Is this a candidate for PII minimization?	◯ Yes ◯ No
Reviewer Notes		
6	Does the PIA accurately identify data retention procedures and records retention schedules?	◯ Yes ◯ No
Reviewer Notes		
7	Are the individuals whose PII is in the system provided appropriate participation?	◯ Yes ◯ No
Reviewer Notes		
8	Does the PIA raise any concerns about the security of the PII?	◯ Yes ◯ No
Reviewer Notes		
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	◯ Yes ◯ No
Reviewer Notes		
10	Is the PII appropriately limited for use internally and with third parties?	◯ Yes ◯ No
Reviewer Notes		
11	Does the PIA demonstrate compliance with all Web privacy requirements?	◯ Yes ◯ No

Save

	Reviewer Questions	Answer
Reviewer Notes		
12	Were any changes made to the system because of the completion of this PIA?	◯ Yes ◯ No
Reviewer Notes		
General Comments		
OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S DN: c=US, o=U.S. Government, ou=HHS, ou=CDC, ou=People, 0.9.2342.19200300.100.1.1=1001440343, cn=Beverly E. Walker -S Date: 2015.02.20 13:17:52 -05'00'	HHS Senior Agency Official for Privacy