Save

Privacy Impact Assessment Form

v 1.47.4

Status Draft Form Number F-29036 Form Date 4/23/2018 8:38:02 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-2243716-158970
2a	Name:	CDC OID Laboratory Response Network Web Application (LRN)
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: Senior Advisor for Preparedness POC Name: Sherrie Bruce POC Organization: CDC/OID/NCEZID POC Email: smb3@cdc.gov POC Phone: 404-639-0474
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	January 18, 2019 □ Not Applicable

Save

11	Describe the purpose of the system.	The laboratory response network (LRN) is a network of public health, military, veterinary, and food testing laboratories that provides laboratory diagnostics and disseminated testing capacity to support public health preparedness and response to an act of bioterrorism, chemical terrorism and other public health emergencies. This system, CDC OID Laboratory Response Network Web Application (LRN), is a communication tool for LRN members. It contains data useful in prevention preparedness and response activities, providing laboratory referral information for locating the nearest neighboring lab during an emergency, agent protocol information, and awareness information to stay current on preparedness and response needs.
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.)	This system facilitates prevention preparedness and response activities. Procedures, reagent ordering, interactive training, and laboratory capacity information are available via LRN Web Application. The system captures the user's name, work phone, work email, and facility location. Once assigned by the Administrator, User IDs are stored in the system permanently. Passwords are encrypted and stored permanently. The User IDs and passwords are used for user authentication only.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The Laboratory Response Network (LRN) is a diverse network of public health, military, veterinary, and food testing laboratories, both domestic and international. It provides laboratory diagnostics and disseminated testing capacity to support public health preparedness and response to an act of bioterrorism, chemical terrorism and other public health emergencies. The LRN Web Application contains data useful in prevention preparedness and response activities, providing laboratory referral information for locating the nearest neighboring lab during an emergency, agent protocol information, and awareness information to stay current on preparedness and response needs. It allows users to view protocol documents, order inventory items, view communications and receive emails from LRN users, broadcast announcements and communicate to the LRN. The system facilitates prevention preparedness and response activities. Procedures, reagent ordering, interactive training, and laboratory capacity information are available via LRN Web Application. The system captures the user's name, work phone, work email, and facility location. User credentials are required for authentication and are stored permanently.
14	Does the system collect, maintain, use or share **PII**?	● Yes ○ No

Save

15	Indicate the type of PII that the system will collect or maintain.	☐ Social Security Number ☒ Name ☐ Driver's License Number ☐ Mother's Maiden Name ☒ E-Mail Address ☒ Phone Numbers ☐ Medical Notes ☐ Certificates ☐ Education Records ☐ Military Status ☐ Foreign Activities ☐ Taxpayer ID User password User ID ☐ Date of Birth ☐ Photographic Identifiers ☐ Biometric Identifiers ☐ Vehicle Identifiers ☐ Mailing Address ☐ Medical Records Number ☐ Financial Account Info ☐ Legal Documents ☐ Device Identifiers ☐ Employment Status ☐ Passport Number
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?	500-4,999
18	For what primary purpose is the PII used?	User credentials (user ID and password) are used for user authentication and authorization. Email, phone number, and name are used for system registration.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	Contact information is also used by CDC to contact LRN members during an event or outbreak.
20	Describe the function of the SSN.	N/A
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.	42 USC 241, Public Health Service Act
22	Are records on the system retrieved by one or more PII data elements?	○ Yes ● No

Save

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.	0920-0850, expires 04/30/2019
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.	When users apply to access the system the first time, users are required to register as users of the system. On the registering web page, users are notified that their business contact information are required and be collected in order to register to the system.
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.	The user business contact information is required to register for the system. If users would like to opt-out of collection of their business contact information (PII), users may choose not to fill out the information on the registering web page. However, if users choose to opt-out, they will not able to access the LRN system.
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.	The individual's business email will be used to notify and obtain consent from the individuals whose business contact information is in the system when major changes occur to the system.

Save

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.	Individual may contact LRN support team through email (LRN@cdc.gov) to resolve an individual's concerns when they believe their business contact information has been inappropriately obtained, used, or disclosed, or that the business contact information is inaccurate. Also, individuals may log into the system to modify or correct their own profile.	
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.	There is no process in place for periodic reviews of the business contact information contained in the system to ensure the data's integrity, availability, accuracy and relevancy. The users' business contact information (PII) is entered by individuals themselves and they may change and manage their own business contact information when they log onto the LRN system. There is no way for LRN team to ensure the data's integrity, availability, accuracy and relevancy, since user may change their own business contact information.	
31	Identify who will have access to the PII in the system and the reason why they require access.	□ Users	
		☒ Administrators	Application administrators have access to user's profile in order to monitor, audit data changes.
		☒ Developers	Developers have access to user's profile to assist the customer with dynamic reports or issues that may arise within the system.
		□ Contractors	
		□ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role based access is in place through assignment of Database access rights governed/approved by the Applications Hosting Branch (AHB). Administrators and developers will only access the web application if the program identifies a potential problem with the data received.	
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.	Least privilege, Role Based Access methods are in place to allow those users only access to their own business contact information and make modifications as needed.	
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 LRN system owners, managers, administrators, technicians, and contractors receive annual security and privacy awareness trainings.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Role-based training is also provided.	
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	● Yes ○ No	

Save

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. Record copy of study reports are maintained in agency from two to three years in accordance with retention schedules. System data, including user's business contact information, is maintained for 20 years or no longer needed. 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. LRN system adheres to the CDC Records and Retention schedule GRS 20.2c, 20.2d, and GRS 20.6
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative controls include Federal, HHS, and CDC specific Privacy, Risk Assessment, and Incident Management Policies, annual system privacy impact assessments; and mandatory annual security & privacy awareness training. Technical controls include application level role based access controls; encryption of sensitive information, including user's business contact information, at rest and in transit; standard baseline configurations for IT assets; server audit and accountability measures; and continuous monitoring of system resources to identify vulnerabilities and ensure adherence to organizationally defined minimum security requirements. Physical controls surrounding the system's data centers include gated campuses with 24-hour guards to enforce access restriction; key card access to campus buildings; and access control lists further limiting physical access to sensitive areas such as the data centers.

General Comments	
OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2019.01.10 19:37:39 -05'00'