Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-13154 | Form Date: 9/19/2017 7:49:30 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-6410927-737605
2a	Name:	OID Infectious Diseases Enterprise LIMS (ID ELIMS)
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.	Implementation
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: James Tolson POC Organization: CDC/OID/OD POC Email: Jst2@cdc.gov POC Phone: 404-639-4224
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	September 29, 2017 ☐ Not Applicable

Save

11	Describe the purpose of the system.	OID Infectious Diseases Enterprise LIMS (ID ELIMS) is the CDC's National Center for Emerging and Zoonotic Infectious Disease (NCEZID) implementation of an Enterprise level Laboratory Information Management System (LIMS). ID ELIMS will facilitate specimen tracking and data management among CDC and its State and local partners. ID ELIMS improves capability for CDC laboratories to prepare for, identify and respond to public health events, reference testing requests and inquiries about specimens tested at CDC; strengthens surveillance and support of epidemiology and laboratory science efforts; tracks specimens securely; improves laboratory data quality and security; prepares readiness for electronic test order and result (ETOR) exchange with external partners; and improves accuracy for electronic health records (EHR). ID ELIMS tracks all incoming specimens to CDC ID laboratories , manages lab specimens tests and data workflows within CDC labs; and produces standard format report for all lab tests to internal and external CDC customers.
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.)	ID ELIMS primarily collects information on laboratory samples submitted to CDC for testing which includes information related to patient demographics, information about the specimen sent to CDC for testing, and any previous testing results. When laboratory samples arrive at CDC, a unique CDC assigned specimen and aliquot identification numbers are assigned and recorded in the system; other metadata collected include publicly available information about the submitting organization, patient history (i.e. illness, infection), patient travel history, exposure history, immunization history, and previous laboratory results. System users are required to access ID ELIMS using user name and password to authenticate via Lightweight Directory Access Protocol (LDAP), when logging in while in the CDC laboratory; however, when accessing the system on CDC office computers, ID ELIMS users are required to login using their PIV card credentials. Log-in credentials are not stored within ID ELIMS, but instead are managed and stored centrally within the CDC server environment.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	ID ELIMS is the unified laboratory information management platform used by the ID laboratories for specimen management and testing. The goals of the LIMS Project are to provide a ID Enterprise system of specimen tracking and data management which can electronically interoperate with CDC, State and local partners LIMS systems. ID ELIMS is being implemented as a laboratory information management system (LIMS) and enterprise resource planning tool that will manage multiple aspects of laboratory informatics as well as support a modern laboratory's operations. Key features include, but are not limited to, laboratory workflow and specimen testing, data tracking support, and data exchange interfaces. The primary information collected by the system includes information related to and describing a specimen that was created in-house, or collected and sent to CDC by its external partners. In addition to this specimen information, additional information may include publicly available submitter information, patient medical records data and laboratory testing results. The system is designed to maintain these records, as well as maintain and store CDC laboratory test results pertaining to these specimens. The ELIMS data will be used by the epidemiologists and laboratorians for public health surveillance and outbreaks, as well as identifying disease trends. In addition, due to the system being used to manage the laboratory, the system also maintains information related to laboratory document control, equipment management, reagent management, and specimen storage locations. The results from the CDC testing along with all of the other information is permanently stored in the system and traceability (audit history records) allow for tracking and tracing of the specimen information. The system will share the lab test results only with the specimen submitters.
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 ☒ 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?	100,000-999,999
18	For what primary purpose is the PII used?	The primary use of PII data in this system is to enable the State public health submitters to identify the submitted sample against the testing results in order to provide patient care or for use during a public health response.
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
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 grant assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)).

Save

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:	09-20-0106, Specimen Handling for Testing and Related Data
		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.		The OMB package is in development. In 2011 the OMB package was determined to be exempt; we are currently reevaluating this.
24	Is the PII shared with other organizations?		(•) Yes ( ) No

Save

24a	Identify with whom the PII is shared or disclosed and for what purpose.	☒ Within HHS Sharing/disclosure of PII data occurs within HHS for the purpose of reporting or communicating the laboratory testing results for a specific patient and/or specimen only in those instances where the Agency is the original submitter. ☒ Other Federal Agency/Agencies PII data is shared with the other Federal Agencies for the purpose of reporting or communicating the laboratory testing results specific patient and/or specimen when they are the original submitter. ☒ State or Local Agency/Agencies Sharing/disclosure of PII data occurs with the State or Local Agencies for the purpose of reporting or communicating the laboratory testing results specific patient and/or specimen when they are the original submitter. ☐ Private Sector
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)).	N/A. Entities and organizations only receive reports on cases they originally submitted, and any PII included is information they themselves provided.
24c	Describe the procedures for accounting for disclosures	All disclosures are tracked via a spreadsheet and must be approved in writing by the specimen owner, laboratory Team Lead, and the ELIMS Science Advisor.
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 process for CDC to notify individuals that their personal information will be collected, because CDC does not directly collect the data but receives it from a third party (State Public Health Lab, other Federal Agencies, International Institutions, and Peace Corp.) The notification process for individuals is the responsibility of the specimen submitters.
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 opt-out of the collection or the submission of PII is determined by CDC Public Health Partners (State Public Health Labs, other Federal Agencies, International Institutions, and Peace Corp.). The opt-out process is the responsibility of our CDC Public Health Partners.

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.	PII data are collected by State Public Health laboratories who submitted to CDC in support of Public Health laboratory testing, outbreaks, surveillance, and investigation activities. In the event a major system change that significantly alters the disclosure and/or use of PII maintained in the system, CDC will notify the State Public Health Partners (State Public Health Labs, other Federal Agencies, International Institutions, and Peace Corp.) of the change so that they can take appropriate action to notify and obtain consent from the affected individuals.	
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.	If there is a PII incident where an individual believes their data has been compromised or is inaccurate, they would contact the third party agency (state health departments) that collected their information prior to contacting the CDC. The CDC official specified in the SORN would be contacted by the State Health Departments. In the case of a discrepancy, the submitter must provide identification and be able to reasonably identify the record and specify the information being contested, the reasons for requesting the correction, and the corrective action sought along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant. The CDC official will work with the CDC testing laboratory to investigate and resolve the data security issue or discrepancy. CDC will then report back to the individual following a successful resolution with the Public Health Agency submitter.	
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.	No system-level process is in place for periodic reviews of PII for data integrity, availability, accuracy and relevancy. ID ELIMS provides laboratory units access to review all data including PII. As the data owners, the laboratories can conduct their own reviews as needed or as consistent with their existing policies.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Specimen data entry, analytical results entry, reporting
		☒ Administrators	Administrators have access to PII data in ELIMS for troubleshooting, database and system management.
		☐ Developers	
		☐ Contractors	
		☒ Others	HHS/CDC badged contractors are used on this project for maintenance and user support and may incidentally view PII data to help troubleshoot user's

Save

32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	In determining which system users may access PII, a role-based access approach is to be used that incorporates audit trails and traceability functions. As a result, access to this system's data is based on the "need to know". Access to PII data is limited to the technical support staff who may incidentally view PII data while assisting users and troubleshoot issues in ID ELIMS. Administrative staff such as the ELIMS database and system administrator have access to PII data through the management the database and application servers. All of the other ID ELIMS team members, such as project managers, developers, LIMS implementation specialists, testers, and trainers only have access to the system's development, testing, and training environments that do not contain PII data.
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.	ID ELIMS utilizes a security rights model that allows CDC administrators to limit individual roles and rights. CDC administrators create unique profiles for each user and assign users to groups and determine controls and clearance levels associated with each user and group (e.g. User 1 associated with Lab A can only access specimen data and its PII that is associated with Lab A; User 1 will not see data associated Lab B). Specific data permissions include access rights to edit/add/delete. A user's role or group controls access to specific ELIMS modules and functionality.
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 ID ELIMS users receive Security and Privacy Awareness Training at least annually.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	All ID ELIMS users receive Role-Based Training. In addition, each user must sign a Rules of Behavior prior to system access.
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.	The specific records retention schedules applicable to the retention and destruction of this data are: CDC RCS, B-321, 2&4; GRS 20.6; and GRS 20.2a.4, 20.2d, and 20.6. Final reports and substantive reporting materials are maintained permanently (CDC RCS, B-321, 2&4). Routine reports are maintained for five years (GRS 20.6). Other input/output records are disposed of when no longer needed (GRS 20.2a.4, 20.2d, and 20.6). 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.

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Only authorized CDC staff, contractors, and guest researchers have access to the data, all of whom receive the appropriate Privacy and role-based trainings prior to access. No data will be allowed to be downloaded to or to reside on a portable device (e.g. laptops, thumb drives, storage media). PII is secured in the system via FISMA compliant Management, Operational, and Technical controls documented in the systems security authorization package. For example, Management Controls include Federal, HHS, and CDC specific Privacy, Risk Assessment, and Incident Management Policies, as well as, annual system privacy impact assessments; 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. 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. Physical security is provided by housing ID ELIMS servers in a secured facility protected by guards and a cardkey system. Access to the computer room is controlled by a PIV card and security code (numeric keypad) system. Access to the data entry area inside of the lab buildings, the laboratories themselves, and offices near the laboratories is controlled by a PIV card.
General Comments		
OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S	Digitally signed by Beverly E. Walker -S Date: 2017.12.04 11:24:15 -05'00'