Save

Privacy Impact Assessment Form

v 1.47.4

Status: Redraft | Form Number: F-78730 | Form Date: 12/21/2020 1:00:09 PM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-6341827-623223
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.	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: 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	2/18/2021 12:00:00 AM ☐ Not Applicable

Save

11	Describe the purpose of the system.	The OID Infectious Diseases Enterprise LIMS (ID ELIMS) is a centralized Laboratory Information Management System
	Question 11 Comments	Please list and spell out the system name first time used.
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 ID ELIMS system collects data from State Agencies the following information: Patient Demographics (Name, DOB, Email Address, Medical Record Numbers, Patient Ids, Age, Illness Onset Date and Gender), Ordering Provider and Organization (Provider name, email Address, National Provider Identifiers, and Organization Identifiers), Lab Performing the tests, Test Ordered by requesters, Test Performed, Results reported in ID ELIMS, Specimen details, Lab Result Medical Notes, and Information obtained from any ask at order entry (AAOE) questions. The data above is provided to the states agencies to match the information submitted with samples as testing results are returned. This is used to properly identify the samples at the state agencies. Users(internal only) authenticate to the ID ELIMS system via Microsoft Active Directory, it has own system boundary and system system authorization, with a Personal Identity Verification (PIV) card.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The OID Infectious Diseases Enterprise LIMS (IDELIMS) is a centralized Laboratory Information Management System (LIMS). The system records, tracks and reports information
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 ☒ 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 Age Gender
	Question 15 Comments	Per Q12 and Q13, Age and Gender is also collect by the system. Please list in the free text "Age and Gender".
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?	PII is used only to uniquely identify specimen and patient information, which we provide back to the submitter as verification as to the correct specimen submitted and tested. The primary use of PII data in ELIMS is the State Public Health submitters can accurately match the submitted sample with the testing results performed by CDC for patient care or a public health response. For some of our laboratory testing, the types of tests that are performed, and the interpretation of these results can be impacted by the PII information that is known and collected. The PII data is provided in the laboratory reports back to the submitting Public Health Agency. In addition CDC Clinical Laboratory Improvement Amendments (CLIA) laboratories are required by regulation to collect at least 2 specific PII data elements, examples of that include patient ID, name and DOB.

Save

19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	The secondary uses for which the PII includes other communications such as telephone, where CDC and the submitting Public Health Agency need to use PII information to convey additional information about a laboratory research and testing methods for a specific patient, specimen or interpretation of the results of a test.	
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)).	
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	

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.	
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 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

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)).	N/A. Some PII is included in reports sent back to the original submitters. However, these 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	Data reporting disclosures are tracked by the audit/traceability functionality provided by the ELIMS system. All other disclosures such as Freedom of Information Act (FOIA) and legal requests 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.	Processes in place for obtaining PII are controlled outside of this agency by submitters of specimen data.
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 information collected is from State and Local Public Health departments, which are mandated as reportable to the departments by local regulations. If an individual choose to opt-out they would provide that information to the State or Local Public Health Department.
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.	Patient PII data are collected by State Public Health laboratories and are submitted to CDC in support of Public Health surveillance, investigation, and intervention activities. In the event a major system change significantly alters the disclosure and/or use of PII maintained in the system, CDC will notify the State Public Health laboratories of the change so they can take appropriate action to notify and obtain consent from the affected individuals. However, notification is unlikely because the HIPAA Privacy Rule, "expressly permits disclosures without individual authorization to public health authorities authorized by law to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to public health surveillance, investigation, and intervention." (HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services, available online at http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm)
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.	Patient PII data are collected by State Public Health laboratories and are submitted to CDC in support of Public Health surveillance, investigation, and intervention activities. CDC has no direct involvement in the PII collection process or contact with the individuals. Therefore, CDC relies upon State Public Health laboratories to have appropriate processes and procedures in place to resolve individual concerns regarding the accuracy and handling of the PII prior to submission. Concerns regarding CDC's use and disclosure of PII are handled according to CDC's PII Incident Response Standard maintained by the Cybersecurity Program Office (CSPO).

Save

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 ELIMS-level process is in place for periodic reviews of PII for data integrity, availability, accuracy and relevancy. 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. ELIMS does not have the authority to mandate a review.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Users will have access for specimen data entry, analytical results entry, and reporting.
		☒ Administrators	Administrators have access to PII data in ELIMS for troubleshooting, database and system management.
		☒ Developers	(Limited) System functional development
		☒ Contractors	Direct contractors are used on this project for maintenance and user support and may incidentally view PII data to help troubleshoot user's
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Accessing ID ELIMS data is provided via Role based access with approval from the Business Steward (BS). Accessing PII data is limited to the technical support staff who may incidentally view PII data while assisting internal users and troubleshoot issues in ID ELIMS. Role-based system access, audit trail and traceability. Administrator have access to system management and troubleshooting; developers do (limited) system functional development; and contractors are used for project design, development, configuration, customizing and maintenance.	
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.	D ELIMS utilizes the Least Privilege Model for granting access to system data. CDC administrators create unique profiles for each user and assign users to groups and determine controls and background 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 IDELIMS users receive Security Awareness Training.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	All IDELIMS users receive Role-Based Training.	
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.	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.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Physical Safeguards: Access to the CDC Clifton Road facility where the mainframe computer is located is controlled by a cardkey system. Access to the computer room is controlled by a cardkey and security code (numeric keypad) system. Access to the data entry area is also controlled by a cardkey system. The hard copy records are kept in locked cabinets in locked rooms. The local fire department is located directly next door to the Clifton Road buildings. The computer room is protected by an automatic sprinkler system, automatic sensors (e.g., water, heat, smoke, etc.) are installed, and portable fire extinguishers are located throughout the computer room. The system is backed up on a nightly basis with copies of the files stored off site in a secure fireproof safe. The 24-hour guard service in buildings provides personnel screening of visitors. Electronic anti-intrusion devices are in effect at the Federal Records Center. Administrative Safeguards: Protection for computerized records both on the mainframe and the Local Area Network (LAN) includes programmed verification of valid user identification code and password prior to logging on to the system, mandatory password changes, limited log-ins, virus protection, and user rights/file attribute restrictions. Password protection imposes user name and password log-in requirements to prevent unauthorized access. Each user name is assigned limited access rights to files and directories at varying levels to control file sharing. There is routine daily backup procedures and secure off-site storage is available for backup tapes. To avoid inadvertent data disclosure, “degaussing” is performed to ensure that all data are removed from Privacy Act computer tapes and/or other magnetic media. Additional safeguards may be built into the program by the system analyst as warranted by the sensitivity of the data. Technical Safeguards: The ID ELIMS system is behind firewalls and intrusion detection system to protect the data at rest. Encryption is in place to protect the data in transit as well as the database the data at rest.

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	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2020.12.28 11:17:56 -05'00'	HHS Senior Agency Official for Privacy