Save

Privacy Impact Assessment Form

v 1.47.4

Status Draft | Form Number F-21315 | Form Date 9/5/2018 1:24:27 PM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-9039673-368482
2a	Name:	ID Enterprise LIMS - Interoperability HL7 Messaging (ID ELIMS HL7)
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: Wendi Kuhnert-Tallman POC Organization: CDC/OID/OD POC Email: Wdk1@cdc.gov POC Phone: 404-639-3103
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	December 5, 2018 ☐ Not Applicable

Save

11	Describe the purpose of the system.	ID Enterprise LIMS - Interoperability HL7 Messaging (ID ELIMS HL7) is the unified laboratory information management platform used by the infectious diseases laboratories for specimen management and testing. ID ELIMS HL7 provides an infectious disease enterprise system of specimen tracking and data management which can electronically interoperate with CDC, State and local partners' enterprise Laboratory Information Management System (LIMS) systems. Its implementation improves patient care as well as public health surveillance and response.
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 HL7 collects the following data from another system, ID ELIMS (ESC# 1188), which has its own PIA: Patient Demographics (Name, DOB, Address, Medical Record Numbers, Patient Ids, Age, Illness Onset Date and Gender), Ordering Provider and Organization (Provider name, 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. Internal staff connect to the system via PIV and Active Directory (AD). AD is a separate system with its own PIA form.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The ID ELIMS HL7 system is used to provide lab test result data to State Public Health submitters. State Health partners accurately match the submitted samples with the testing results performed by CDC for patient care or a public health response. The testing results contains PII data elements that is retrieved from the system ID ELIMS (ESC# 1188) . The PII data elements included : Patients Demographics (Name, DOB, Address, Medical Record Numbers, Patient Ids, Age, Illness Onset Date and Gender), Ordering Provider and Organization(Provider name, Address, National Provider Identifiers, and Organization Identifiers) , Diagnostic Lab, Test ordered, Test Performed, the results in ID ELIMS, Specimen details, lab results medical notes, and ask at order entry (AAOE) information. 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 Public Health Partner agencies. Internal staff connect to the system using PIV credentials with authentication via Active Directory (AD). AD is a separate access system with its own PIA.
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 Gender Age ☒ 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 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.
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 testing method 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

Save

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	
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 ☒ Other Federal Agency/Agencies PII data is shared with the other Federal Agencies submitters for the purpose of reporting or communicating the laboratory testing results specific patient and/or specimen. ☒ State or Local Agency/Agencies PII data is shared with the State or Local Public Health Agency submitter for the purpose of reporting or communicating the laboratory testing results for a specific patient and/or specimen. ☐ 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
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 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.	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.	CDC does not have an opt out process because it does not directly collect the data but receives it from a third party. Any opt-out methods would be implemented by said third party (State Public Health Labs, other Federal Agencies, International Institutions, and Peace Corp.).
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 they can take appropriate action to notify and obtain consent from the affected individuals.

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.	If there is a PII incident where an individual believes their data has been compromised or is inaccurate, they would contact the CDC official specified in the SORN. The CDC Official will work with the CDC testing laboratory to investigate and resolve the data security issue or discrepancy. CDC would facilitate the resolution based on the individual's request and report back to the individual following a successful resolution with the Public Health Agency submitter. 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.
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: 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: Direct contractors are used on this project for maintenance and user support and may incidentally view PII data to help troubleshoot user's
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Accessing ID ELIMS HL7 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
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 HL7 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 with 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 and Privacy Awareness Training at least annually.

Save

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
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 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 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 HL7 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 at rest.

Save

General Comments	
OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2018.10.17 19:53:54 -04'00'