

Privacy Impact Assessment Form

v 1.21

Status

Form Number

Form Date

06/28/21

Question

Answer

1 OPDIV:

CDC

2 PIA Unique Identifier:

TBD

2a Name:

NCEH DLS Laboratory Quality Assurance Programs

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

Deputy ADS

POC Name

Yan (Shirley) Ding

POC Organization

DLS, NCEH

POC Email

yad6@cdc.gov

POC Phone

7704887934

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

☒ Not Applicable

8c	Briefly explain why security authorization is not required	The program uses multiple CDC authorized systems for information collection, storage, and processing.
10	Describe in further detail any changes to the system that have occurred since the last PIA.	None
11	Describe the purpose of the system.	The Division of Laboratory Sciences (DLS) provides samples and technical assistance to laboratories to improve the quality and accuracy of tests. Some DLS quality assurance (QA) programs provide certification for proficiency of testing (PT). Some DLS QA programs are intended to ensure accurate and consistent test results across multiple laboratories (i.e. Standardization/Harmonization).
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 program will collect and maintain the following information: laboratory (laboratory name, organization, program name, address, phone number, etc.), user (name, title, email), sample (sampleID, analyte, instrument, protocol, analyte concentration, sequence, analysis date, reagent lot, calibrator lot, etc.), and analysis (differential between expected and reported values, suggested remediation, etc.).
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	<p>Laboratories use DLS-developed samples to test the quality and accuracy of their methods/assays. Participating laboratories enroll in the DLS QA program that fits their needs (proficiency testing, certification, general quality assurance or accuracy-based monitoring, standardization, etc.). After the laboratories receive DLS QA samples and perform their methods, they return test results to DLS. DLS then evaluates the data using statistical methods and reports back to the laboratories on their performance.</p> <p>Laboratory information is used to identify a specific laboratory, reduce duplicates, and send correspondence. This information is not shared. These data are collected from participating laboratories.</p> <p>User information is needed to distribute lab results and certificates of the proficiency testing, and to contact the lab when there are problems with samples or questions about submitted data. These data are collected directly from users in participating laboratories.</p> <p>Sample information is needed to compare values obtained in the participating national and international labs versus the accepted values from the standards that were sent to the labs. Only de-identified, aggregate information is shared with all participating labs. These data are collected from participating laboratories.</p> <p>Analysis information is used to improve the accuracy of lab results from the participating labs. This information is shared only with the lab to which the analysis and data pertains.</p>
14	Does the system collect, maintain, use or share PII?	<input checked="checked" type="radio"/> Yes <input type="radio"/> No

15	Indicate the type of PII that the system will collect or maintain.	<div> <input type="checkbox"/> Social Security Number <input type="checkbox"/> Date of Birth </div> <div> <input checked="" type="checkbox"/> Name <input type="checkbox"/> Photographic Identifiers </div> <div> <input type="checkbox"/> Driver's License Number <input type="checkbox"/> Biometric Identifiers </div> <div> <input type="checkbox"/> Mother's Maiden Name <input type="checkbox"/> Vehicle Identifiers </div> <div> <input checked="" type="checkbox"/> E-Mail Address <input checked="" type="checkbox"/> Mailing Address </div> <div> <input checked="" type="checkbox"/> Phone Numbers <input type="checkbox"/> Medical Records Number </div> <div> <input type="checkbox"/> Medical Notes <input type="checkbox"/> Financial Account Info </div> <div> <input type="checkbox"/> Certificates <input type="checkbox"/> Legal Documents </div> <div> <input type="checkbox"/> Education Records <input type="checkbox"/> Device Identifiers </div> <div> <input type="checkbox"/> Military Status <input type="checkbox"/> Employment Status </div> <div> <input type="checkbox"/> Foreign Activities <input type="checkbox"/> Passport Number </div> <div> <input type="checkbox"/> Taxpayer ID <input type="text" value="Other..."/> </div> <div> <input type="text" value="Other..."/> <input type="text" value="Other..."/> </div> <div> <input type="text" value="Other..."/> <input type="text" value="Other..."/> </div>
16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	<input type="checkbox"/> Employees <input type="checkbox"/> Public Citizens <input checked="" type="checkbox"/> Business Partners/Contacts (Federal, state, local agencies) <input type="checkbox"/> Vendors/Suppliers/Contractors <input type="checkbox"/> Patients Other <input type="text"/>
17	How many individuals' PII is in the system?	<input type="text" value="100-499"/>
18	For what primary purpose is the PII used?	<input type="text" value="To distribute lab results and certificates of the proficiency testing."/>
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	<input type="text" value="To contact the laboratory about issues with a sample or questions with submitted data."/>
20	Describe the function of the SSN.	<input type="text" value="N/A"/>
20a	Cite the legal authority to use the SSN.	<input type="text" value="N/A"/>
21	Identify legal authorities governing information use and disclosure specific to the system and program.	<input type="text" value="Section 301 of the Public Health Service Act (42 U.S.C.241)"/>
22	Are records on the system retrieved by one or more PII data elements?	<input type="radio"/> Yes <input checked="" type="radio"/> 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.	<div>Published: <input type="text" value="N/A"/></div> <div>Published: <input type="text"/></div> <div>Published: <input type="text"/></div> <div><input type="checkbox"/> In Progress</div>

23	Identify the sources of PII in the system. <div style="margin-left: 20px;"> Directly from an individual about whom the information pertains <input type="checkbox"/> In-Person <input checked="" type="checkbox"/> Hard Copy: Mail/Fax <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> Online <input type="checkbox"/> Other Government Sources <input type="checkbox"/> Within the OPDIV <input type="checkbox"/> Other HHS OPDIV <input type="checkbox"/> State/Local/Tribal <input type="checkbox"/> Foreign <input type="checkbox"/> Other Federal Entities <input type="checkbox"/> Other Non-Government Sources <input type="checkbox"/> Members of the Public <input type="checkbox"/> Commercial Data Broker <input type="checkbox"/> Public Media/Internet <input type="checkbox"/> Private Sector <input type="checkbox"/> Other </div>
23a	Identify the OMB information collection approval number and expiration date. <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">OMB package is in preparation</div>
24	Is the PII shared with other organizations? <div style="margin-left: 20px;"> <input type="radio"/> Yes <input checked="" type="radio"/> No </div>
24a	Identify with whom the PII is shared or disclosed and for what purpose. <div style="margin-left: 20px;"> <input type="checkbox"/> Within HHS <input type="checkbox"/> Other Federal Agency/Agencies <input type="checkbox"/> State or Local Agency/Agencies <input type="checkbox"/> Private Sector </div>
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)). <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">Information will not be disclosed or shared.</div>
24c	Describe the procedures for accounting for disclosures <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">Disclosures are not planned. However, if a disclosure needs to be made, they will be accounted for in a spreadsheet that is maintained by the study data manager and principal investigator.</div>
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. <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">There is no process in place to notify individuals that their data will be collected. Users of the system will provide their name and email in order to gain access to the system.</div>
26	Is the submission of PII by individuals voluntary or mandatory? <div style="margin-left: 20px;"> <input checked="" type="radio"/> Voluntary <input type="radio"/> Mandatory </div>

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.	Individuals may opt-out of providing their PII. However, they will not be able to use the system if they opt-out.
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.	Individuals will be contacted by email if major changes occur to the system.
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.	Individuals may contact the program using the email or phone number on the website if they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. The program will respond to the concerns and correct the issues.
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.	The program will check with the laboratories to ensure that current users are authorized to access the system. Individuals will be contacted annually to verify their PII in the system.
31	Identify who will have access to the PII in the system and the reason why they require access.	<div> <input checked="" type="checkbox"/> Users <div>Create, edit, delete, view records and reports</div> </div> <div> <input checked="" type="checkbox"/> Administrators <div>Create new users and assign user roles</div> </div> <div> <input type="checkbox"/> Developers <div></div> </div> <div> <input type="checkbox"/> Contractors <div></div> </div> <div> <input type="checkbox"/> Others <div></div> </div>
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role-based access is in place. Users are authenticated by multiple CDC authorized systems including active directory, and only administrators will have access.
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 applied. Managers can only view PII for CDC employees who report to them within each module. Managers can only access PII after having the managerial group permission associated to their account by the system business steward.
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.	CDC security awareness training will be provided to all internal users.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Role-based training is provided to internal and external users of the system.
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	<input checked="" type="radio"/> Yes <input type="radio"/> No

<p>37 Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.</p>	<p>PII in the system will be retained according to the Scientific and Research Project Records, Records Control Schedule, 3. Minor Research Records. Records are maintained at least six years, but no longer than ten years, after the retirement of the system—depending upon program need for scientific, legal, or business reference—then deleted/destroyed.</p>	
<p>38 Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.</p>	<p>The administrative controls educate system users of their responsibility to protect PII and legally bind them to do so. These controls include signed rules of behavior, non-disclosure agreements, CDC privacy and security awareness training, and records management training. Records are maintained according to CDC record control policies and procedures.</p> <p>The technical controls, implemented by the system, act to either allow access to system PII data only to approved users or to make PII data unreadable outside of the system. These controls include encryption, authentication, firewalls, intrusion detection systems, and anti-malware systems.</p> <p>The physical controls, implemented by the system, restrict access to CDC buildings and areas housing computers used by this system. These controls include guards, identification badges, key cards, locked doors, cipher locks, fences, alarms and closed circuit TV.</p>	
<p>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.</p>		
Reviewer Questions		Answer
1	Are the questions on the PIA answered correctly, accurately, and completely?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
2	Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
3	Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
4	Does the PIA appropriately describe the PII quality and integrity of the data?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
5	Is this a candidate for PII minimization?	<input type="radio"/> Yes <input type="radio"/> No

Reviewer Questions		Answer
Reviewer Notes		
6	Does the PIA accurately identify data retention procedures and records retention schedules?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
7	Are the individuals whose PII is in the system provided appropriate participation?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
8	Does the PIA raise any concerns about the security of the PII?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
10	Is the PII appropriately limited for use internally and with third parties?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
11	Does the PIA demonstrate compliance with all Web privacy requirements?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
12	Were any changes made to the system because of the completion of this PIA?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
General Comments		
OPDIV Senior Official for Privacy Signature		HHS Senior Agency Official for Privacy