Save

Privacy Impact Assessment Form

Status	Draft	Form Number	F-48574	Form Date	1/9/2020 10:18:52 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-4950231-463145
2a	Name:	Quality Assessment Program (QAP)
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: PUBLIC HEALTH ADVISOR POC Name: Jennifer E. Buigut POC Organization: NCEZID POC Email: cko1@cdc.gov POC Phone: 770.488.4552
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	April 2, 2020 ☐ Not Applicable

11	Describe the purpose of the system.	The Quality Assessment Program (QAP) system was developed by the Division of Global Migration and Quarantine (DGMQ), Immigrant, Refugee and Migrant Health Branch to record and track data on over 1,200 panel physicians in over 600 panel sites in various countries to ensure the quality of overseas medical screening examinations for visa applicants. It serves as a repository for site evaluations conducted by DGMQ QAP teams of physicians and laboratorians, who recommend remediation, site removal, training, and/or consultation based on CDC guidelines.
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.)	Information collected includes: (1) For the facility: Latitude and longitude of City's center, Country, State, site visit purpose, facility address, facility email, facility fax, facility name, facility postal code; (2) For the Supervisor: First name last name, middle initial (MI), site address, site email, site fax, site latitude and longitude, site phone; (3) For the Physician: Address, physician cell, physician email, physician fax, physician first name last name, MI, physician postal code, problem, problem report, site visit date, user entering data first name, middle, and user id (not for authentication purposes). QAP does not store user identification or password for access. Authentication is accomplished via Active Directory (AD). AD is a separate system with its own PIA.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	QAP was developed to record and track physician data in over 600 panel sites in various countries to ensure the quality of overseas medical screening examinations for visa applicants. Site visit evaluations are conducted by DGMQ QAP teams of physicians and laboratorians. The site visits are based on the volume of migrants and disease prevalence rates. Information captured during the site visits are compiled into a report also referred to as a Trip Report or Panel Physician Evaluation. Trip Reports are shared within the division and with the respective U.S. Embassy for a particular panel site. The system stores information obtained during these DGMQ site visits, and maintains panel physician and facility evaluations. Information collected includes: (1) For the facility: Latitude and longitude of City's center, Country, State, site visit purpose, facility address, facility email, facility fax, facility name, facility postal code; (2) For the Supervisor: First name last name, middle initial (MI), site address, site email, site fax, site latitude and longitude, site phone; (3) For the Physician: Address, physician cell, physician email, physician fax, physician first name last name, MI, physician postal code, problem, problem report, site visit date, user entering data first name, middle, and user id (not for authentication purposes). QAP does not store user identification or password for access. Authentication is accomplished via Active Directory (AD). AD is a separate system with its own PIA.

14	Does the system collect, maintain, use or share **PII**?	◉ Yes ○ No

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

Fax

User Id

City Longitude and Latitude

Site Longitude and Latitude

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?	PII is obtained to record the Site, Supervisor, Physician, and individual performing the site visit.

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)).

22	Are records on the system retrieved by one or more PII data elements?	○ Yes ⦿ No

23	Identify the sources of PII in the system.	**Directly from an individual about whom the information pertains**

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.	N/A. Information is not collected pursuant to the Paperwork Reduction Act (PRA).

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.	Individuals are asked for their business contact information during the course of the Site Visit and are told that this information is will be included in the site visit report.

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.	Users cannot opt-out of collection of their PII. The information maintained on Panel Physicians is business contact information which is required for other purposes as well, including training announcements, important updates and general communications should questions arise.

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.	Participating Sites will be notified when major changes occur to the system using the contact information on file. The sites can be notified either by phone, email, or with a letter to the physical mailing address. The Point of Contact on this form is responsible for notifying the sites.

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.	Any individual who has concerns may contact the CDC site visit point of contact to resolve any 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.	Consular Sections (US State Department) are required to inform us of any changes to panel physicians within their countries, and we make changes to the database based on those notifications. Panel physicians will also let us know when their contact info has changed for any reason. Through those two mechanisms, the program is regularly updating the database to maintain accuracy based on information received.	

31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Users have access to the data in order to complete the site visit report.
		☒ Administrators	Administrators have access to the data to ensure the quality of the data in the database and add users as determined by the program.
		☒ Developers	Developers have access to the data in order to generate SQL queries for the users and needed.
		☒ Contractors	Users, Developers, and Administrators may be CDC direct contractors. They would have access to the data based on their role as explained above.
		☐ Others	

32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The program first evaluates whether the individual has a need for access to the system. If the individual's manager determines that access to the system is required for the
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 used to allow those with access to PII to only access the minimum amount of information necessary to perform their job. The system administrator is responsible for setting up the user access to the system based on the CDC user id and the permissions assigned to it.
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.	Annual CDC Security Awareness Training (SAT) and Privacy training is mandatory for all CDC system users.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Annual Role Based Security Training is required for IT Administrators.
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.	Records are maintained and destroyed according to the CDC General Records Schedule (GRS) 20.6. Records are maintained in agency for five years. 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. Records are destroyed by paper shredding process when 10 years old, unless needed for further study.

| 38 | Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls. | Administrative - Access to the application is approved by the individuals supervisor indicating that the user has a need to know the information on the system.

Technical - The CDC user id is encrypted while stored in the Active Directory system.

Physical- The server is housed on CDC property with gate security guards at the entrances to the property, individual user access credentials are required for each non-public building , floor, and office. Closed circuit TV is also used by the internal security guards to check for and grant access to authorized individuals. | |

General Comments	

OPDIV Senior Official for Privacy Signature	