Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-74125 | Form Date: 4/25/2019 10:45:40 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-3929910-878547
2a	Name:	EIP Plus Messaging (EIP+M)
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.	Development
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: Alvin Shultz POC Organization: NCEZID/DPEI POC Email: fcu9@cdc.gov POC Phone: 404-639-7028
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	July 19, 2019 ☐ Not Applicable

Save

11	Describe the purpose of the system.	Emerging Infections Program (EIP) Plus Messaging (EIP+M) is a surveillance system that provides transformation and validation of Health Level Seven (HL7) messages to EIP state partners. EIP+M provides transformation and validation of the messages. The messages are made available for display to CDC users and State Partners via a secure Web Portal. EIP+M receives HL7 messages via the Message Validation, Processing, and Provisioning System (MVPS) system. MVPS is a separate CDC system with its own PIA. Messages are routed from MVPS to Association of Public Health Labs (APHL), which is a clearing house broker for HL7 messages. These messages are sent to EIP+M by APHL. EIP+M provides transformation and validation of the messages. The messages are made available for display to CDC users and State Partners via a secure Web Portal.
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.)	EIP+M contains lab results and patient demographics (DOB, State, County, Age, Race, Sex, Zip Code) which is provided to the states agencies to match the information submitted with HL7 samples as testing results are returned. This is used to properly identify the samples at the state agencies. The State Agencies have access to the EIP+M system directly via secure URL, so user ID and password are needed for login. These user credentials are stored permanently on the system.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	EIP+M is a surveillance system that receives HL7 messages via the MVPS system. MVPS is a separate CDC system with its own PIA. Messages are routed from MVPS to APHL, which is a clearing house broker for HL7 messages. These messages are sent to EIP+M by APHL. EIP+M provides transformation and validation of the messages. The messages are made available for display to CDC users and State Partners via a secure Web Portal. The EIP+M system contains lab results and patient demographics (DOB, State, County, Age, Race, Sex, Zip Code). Data elements are secured by restricted access to the secure Web Portal. The EIP+M system contains Patient Demographics (DOB, State, County, Age, Race, Sex, Zip Code). This information is collected and provided to the state agencies to match the information submitted with HL7 samples as testing results are returned. This is used to properly identify the samples at the state agencies. The data collected is used to geographically and demographically locate the incidence of disease and categorize it by the impacted geographic and demographic groups. This information will be used for research purposes to better inform the public on how to prevent and/or treat the disease. The State Agencies have access to the EIP+M system directly via secure URL, so user ID and password are needed for login. These user credentials are stored permanently on the system. Data elements are secured by restricted access to the secure Web Portal. Messages are maintained in a secure, encrypted Structured Query Language Server database. Database maintenance and backups are performed on a regularly scheduled basis.
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 DOB, State, County, Age, Race, Sex, Zip Code Test/lab results user credentials (User ID and Password)
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?	50,000-99,999
18	For what primary purpose is the PII used?	PII is used to geographically and demographically locate the incidence of disease and categorize it by the impacted demographic group. User credentials are needed for access.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	This information will be used for research purposes to better inform the public on how to prevent and/or treat the disease.
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 maintain data and provide 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

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.	OMB Collection Approval 0920-0978, Expires 04/30/22
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 ☐ Other Federal Agency/Agencies ☒ State or Local Agency/Agencies Disease Surveillance and Research ☐ 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	N/A
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.	Prior notice is not given to the individuals because the data is originally provided to CDC by the State and Local Health Departments, and any prior notice would be given by theses entities. CDC collects this data whenever a case is reported by a partner health agency, as required.

Save

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.	There is no option to object to the collection of the information. Local health regulations require these types of confirmed laboratory test results to be reported. The information collected by this system comes from State and Local Public Health departments whenever a case is reported by a partner health agency.
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.	If there were major changes to the system, the program would contact the state health departments. It would not be possible to directly notify and obtain consent from the individuals whose PII is in the system, because the system does not collect any identifiable information that would allow CDC to contact them.
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.	There is not a redress process in place because of the nature of the data that the system maintains; there is virtually no identifiable data. The individual can contact the health facility where the PII was collected, and any redress rights would be exercised at the state and local levels where the information is collected.
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 EIP+M Administrator reviews the overall Messages received and exception logs each morning. Administrative staff such as the EIP+M database and system administrator have access to PII data through the management of the EIP+M database and application servers. Data within the repository will be obtained and reviewed nightly to ensure its integrity, availability, accuracy and relevancy.
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users: Users will have access to PII data for Surveillance and research reporting. ☒ Administrators: Administrators have access to PII data in EIP+M for troubleshooting, database and system management. ☐ Developers ☐ Contractors ☐ Others
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Accessing EIP+M 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 EIP+M. Role based access, audit trail and traceability are implemented. The administrator uses the system admin functionality to grant access to the system based on the role of the user.

Save

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 and 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. User access is limited to job function and information only essential to the user function. Role based access, audit trail and traceability are implemented. The administrator uses the system admin functionality to grant access to the system based on the role of the user.
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 EIP+M personnel 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 EIP+M system users also receive role-based training on an annual basis.
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 retained and disposed of in accordance with the CDC Scientific and Research Project Retention Schedule N1-442-09-1. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative 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 Federal Information Security Management Act (FISMA) compliant Management, Operational, and Technical controls documented in the systems security authorization package. This include Federal, HHS, and CDC specific Privacy, Risk Assessment, and Incident Management Policies, as well as annual PIA reviews. Technical Controls: 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. The implementation uses Advanced Encryption Standard, which is a Federal Information Processing Standards compliant for Server database encryption of the data. Column level encryption is implemented to ensure PII data is secure. Physical Controls: Physical controls included security guards at gate to access facility, card key access and physical locks to data rooms.

Save

General Comments	
OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2019.07.17 11:33:48 -04'00'