Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-48779 | Form Date: 11/25/2019 1:22:19 PM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-8036781-710160
2a	Name:	Epidemic Information Exchange 2.0 (EPi-X 2.0)
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: IT Specialist POC Name: Robert Bohn POC Organization: DDPHSIS/CPR/DEO POC Email: iei8@cdc.gov POC Phone: (404) 718-6431
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	January 31, 2020 ☐ Not Applicable

Save

11	Describe the purpose of the system.	The purpose of the system is to help local, state, and federal public health officials report and discuss outbreaks as these outbreaks are identified, investigated, and reported. Epi-X provides rapid reporting, immediate notification, editorial support, and coordination of health investigations for public health professionals to meet the overarching goals of HHS.
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.)	Epi-X 2.0 will collect, maintain (store), or share health-related data including information about epidemics or potential public health events, and airline passenger data to be used in tracking potential transmission of contagious diseases communicated in flight with the CDC and Federal/state/local and other public health entities. The PII will consist of names, email addresses, phone numbers, medical notes, flight records, dates of birth, mailing address, and employment status. The Epi-X 2.0 system does not collect information (i.e. user credentials) about system users/administrators in order to control access. Access is granted using Active Directory (AD) or the Secure Access Management System (SAMs) which are separate systems covered by separate PIAs.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	Epi-X 2.0 facilitates secure data sharing between CDC and Federal/state/local and other public health entities. Its purpose is to serve as the CDC's secure, moderated, bi-directional method of communicating outbreak and potential terrorist information to state and local health departments, other Federal agencies, and selected international groups and organizations. It is also the preferred method of notifying users of vital time-sensitive public health information. The system provides rapid reporting, immediate notification, editorial support, and coordination of health investigations for public health professionals. Each type of information listed is collected into and/or maintained in the system is health-related data provided by epidemiologists and by the Division of Global Migration and Quarantine (DGMQ). This data is used to report vital public health events that are of national importance, including outbreaks, disasters, and possible terrorism reports. Data provided by epidemiologists includes information not yet released to other sources about epidemics or potential public health events. The DGMQ data is voluntarily-supplied airline passenger data to be used in tracking potential transmission of contagious diseases communicated in flight. This information system serves as the preferred method of notifying users of vital time-sensitive public health information. The PII will consist of names, email addresses, phone numbers, medical notes, flight records, dates of birth, mailing address, and employment status. The Epi-X 2.0 system does not collect information (i.e. user credentials) about system users/administrators in order to control access. Access is granted using Active Directory or the Secure Access Management System (SAMs) which are separate systems covered by separate PIAs. Direct contractors use HHS credentials to access the system; and are members of DGMQ and DEO. Any access or use of the information is intended to notify users of vital time-sensitive public health information rapidly.
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 Flight records
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: International travelers
17	How many individuals' PII is in the system?	5,000-9,999
18	For what primary purpose is the PII used?	Using the PII made available through EPI-X 2.0, authorized public health personnel (users) can collaborate about evolving public health events and the possible causes of outbreaks. This allows users to anticipate, identify, and respond to health problems in their own communities as well as to alert other Epi-X 2.0 users of outbreaks or other health events that might affect their areas. This data output is not exported to another information system within or outside the CDC.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	PII is also used with respect to international travelers (also users) who wish to be notified if they are exposed to disease while traveling aboard aircraft.
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 318B

Save

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:	DHS/FEMA/GOVT-001, Federal Emergency Management Agency National Defense Executive Reserve System.
		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.		N/A
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 To collaborate about evolving public health events and the possible causes of outbreaks. ☐ Other Federal Agency/Agencies ☒ State or Local Agency/Agencies To collaborate about evolving public health events and the possible causes of outbreaks. ☒ Private Sector To collaborate about evolving public health events and the possible causes of outbreaks.
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)).	None
24c	Describe the procedures for accounting for disclosures	Audit logs are used.
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.	Each user is presented with a Rules of Behavior (ROB) document for Epi-X 2.0, known as the Epi-X User Agreement. By consenting to the User Agreement, each user is advised therein that their PII will be collected and made available to other users. ROB recipients must formally acknowledge their understanding and agreement with the rules through electronic signature. ROB recipients are required to consent via electronic notification before they are authorized to use the information system. The information system collects information directly from an individual and this collection is considered to be voluntary. Any data collected by the information system is obtained electronically. However, because an individual has access to the information system, they have been apprised of how the data will be utilized. The information system does not collect PII from another system therefore there are no notices stating such.
26	Is the submission of PII by individuals voluntary or mandatory?	◉ Voluntary ○ Mandatory

Save

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.	If individuals opt-out of the collection or use of their PII, they will not be allowed access. Epi-X 2.0 users who accept access to the system are notified that they will be sharing PII information with other information system users. If a user decides to opt-out of the collection or use of their PII would, their access to Epi-X 2.0 will be revoked. Logical access to Epi-X 2.0 is a voluntary decision of individual users and is not mandatory by the organization. Epi-X 2.0 can only be accessed to users with access to the CDC demilitarized zone (DMZ). Epi-X 2.0 cannot be accessed if the user is not logged onto the CDC internal website. Once a user is inside the CDC DMZ, they can navigate to the Epi-X 2.0 web portal. Role based access controls are in place to assign users to view pages/links within the Epi-X 2.0 system. An Epi-X 2.0 user will receive an error message stating that they do not have permission to view such pages/links.
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.	Any changes within the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection) will be communicated by a member of the CDC Division of Emergency Operations (DEO) Staff Team. During employee orientation, any employee that will be working within the CDC Director's Emergency Operations Center (EOC) or the Epi-X 2.0 Administrative Team will be notified that their PII information will be used in support of the EOC. Acceptable communication methods (ie. email, phone call, in person, etc.) will be at the discretion of the CDC Epi-X 2.0 Administrative Team with the purpose to notify individuals and/or obtain consent for any new uses or disclosure of PII that has been previously collected prior to any new use or disclosure.
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.	An individual who requests access to records shall, at the time the request is made, designate in writing a responsible representative who is willing to review the record and inform the subject individual of its contents at the representative's discretion. Per the SORN 'Contesting Record Procedures', the individual will contact the first official at the address specified under System Manager above, reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

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.	The Epi-X 2.0 account auditing process entails review of user accounts annually by Epi-X 2.0 Administrative Team and Epi-X 2.0 Helpdesk. An annual review of policies governing auditing by the Security Steward, Business Steward, and Technical Steward will also take place. The policy must be signed by the Business Steward, Security Steward and Deputy Director of DEO. This annual account auditing process entails review of Epi-X 2.0 user accounts annually by Epi-X 2.0 Administrative Team and Epi-X 2.0 Helpdesk. Access to Epi-X 2.0 is managed through AD; and users are removed from the system when they are removed from AD. For users whose roles change due to job reassignment or retirement, Epi-X 2.0 Administrative Team and Epi-X 2.0 Helpdesk relies on communication via phone or email to notify that the account needs to modified.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Epi-X 2.0 users have the flexibility to create reports for analysis with data contained within the web portal. All data that is collected and disseminated
		☒ Administrators	Have full access to all data and functions within the system. They are also known as 'Super Administrators'
		☒ Developers	The development team are members of the Epi-X 2.0 Administrative Team and Epi-X 2.0 Helpdesk. If an Epi-X 2.0 user is unavailable or unable to access
		☒ Contractors	These are referred to as 'direct contractors' and are part of the development team.
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Epi-X 2.0 is a role role-based security system to prevent a level of activity without collusion. Role separation is clearly delineated by action to be performed and administrative rights	
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 Epi-X 2.0 web application allows access to PII with the assignment of privileges that will be granted via settings in the Epi-X 2.0 system and set by system administrators. Epi-X 2.0 web application relies upon interfaces to the procuring activity's SAMS system (Secure Access Management System) to control access to role based elements of the interface as SAMS is an authentication mechanism that allows access to the Epi-X 2.0 web application. SAMS does not, in and of itself, guarantee least privilege. Epi-X 2.0 allows access only to an individual's data if an information system has been granted access to the Epi-X 2.0 web application. All access is determined by ACLs.	

Save

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 users are required to take the annual CDC Security Awareness Training (SAT) which covers Security Awareness, Privacy Awareness, Insider Threat, and Counterintelligence information. There is also Epi-X 2.0 User Security Training course that helps students gain an understanding of the importance of security and their responsibilities in maintaining security and confidentiality as defined in the user agreement. Upon completing the course, users will be asked to sign and an Epi-X User Agreement which makes them aware of their responsibilities for protecting the information.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Upon request, users with varying access levels can request specified training to assist them in understanding why security is important for Epi-X 2.0.
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.	The procedures for a system defined as an Epidemiologic Studies and Surveillance of Disease Problems, the 'Retention and Disposal' procedures are to copy the study reports as a record that is to be maintained in agency from two to three years in accordance with retention schedules. Source documents for computer are to be disposed of when they are no longer needed by program officials. 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. 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 recycling process when 20 years old, unless needed for further study. Epi-X 2.0 does not list the Records Control Schedule (RCS) Job Numbers or General Records Schedules (GRSs) applicable as there is no RCS or GRS identified.

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative controls: the Epi-X 2.0 information system has successfully undergone a Security Assessment and Authorization (SA&A) and has acquired an Authorization to Operate (ATO). The SA&A artifacts contain a system security plan which details how the system meets all required security controls per the NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations". Epi-X 2.0 has a tested backup plan which required all information system personnel to review notification processes and adequate training to meet their responsibilities for protecting data that is collected and maintained as part of the aforementioned security plan. Epi-X 2.0 undergoes regularly scheduled backups and there exists offsite backup storage for better operability. Technical controls: all Epi-X 2.0 users have been authorized by system administrators. The Epi-X 2.0 Administrative team and the Epi-X 2.0 Helpdesk members are authorized CDC network account holders that have undergone background checks and identify proofing. To acquire access to the CDC network, the system administrator functions requires an HHS PD-12 compliant PIV card. The Epi-X 2.0 information system database is protected by the CDC perimeter firewall which is further monitored by intrusion detection systems, anti-virus scans, and other network vulnerability scans. Privacy and/or security incidents concerning this system are covered under the CDC Incident Response Plan. Physical controls: the facility that the Epi-X 2.0 information system servers are hosted has multi-layered protection. The protection includes security guards, secure doors requiring proxy card entry pads, and Closed Circuit TV monitors. All personnel must have CDC or HHS Identification Badges or be authorized visitors escorted by CDC staff.
General Comments		
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2019.11.26 12:54:13 -05'00'	