Save

Privacy Impact Assessment Form

v 1.21

Status | Form Number | Form Date

	Question	Answer
1	OPDIV:	CDC/DDPHSS/CSELS
2	PIA Unique Identifier:	
2a	Name:	Epi Info Secure Web Survey - PRA
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 Project Manager POC Name: Leslyn McNabb POC Organization: CDC/OPHSS/CSELS POC Email: axe8@cdc.gov POC Phone: 404-498-2286
7	Is this a new or existing system?	○ New ◉ Existing
8	Does the system have Security Authorization (SA)?	◉ Yes ○ No
8a	Date of Security Authorization	Jun 30, 2020

Save

9	Indicate the following reason(s) for updating this PIA. Choose from the following options.	☒ PIA Validation (PIA Refresh/Annual Review) ☐ Significant System Management Change ☐ Anonymous to Non-Anonymous ☐ Alteration in Character of Data ☐ New Public Access ☐ New Interagency Uses ☐ Internal Flow or Collection ☐ Conversion ☐ Commercial Sources Other...
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 Epi Info Secure Web Survey system (EISWS) allows CDC users with authorized access to the Epi Info system to create, distribute, and receive completed online surveys to gather information for analysis. The surveys can be distributed to the targeted audience using emails or any other electronic form. Each survey is accessed using the URL that is unique to a given survey. An epidemiologist will be able to download the survey responses from web and analyze the survey data any time during the period the survey is open or after the survey has closed using Epi Info desktop application.
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.)	CDC programs use The Epi Info Secure Web Survey system (EISWS) to collect public health data for epidemiologic investigations and research studies. The system will collect data that enables epidemiologists to conduct outbreak investigations, track cases, perform contact tracing, evaluate public health interventions, and collect information on attitudes and behaviors that impact public health outcomes. Programs that use this system must sign an agreement after reading the Rules of Behavior (RoB) document that explicitly indicates the terms and usage of the system and what information can be collected. The data collected may vary dependent upon the unique variables needed by individual research studies. However, any data collected must fall within the parameters of the RoB, and as such is limited to: Name, Date of Birth or Age, Sex, Mailing Address, Physical Address, Physical locations traveled, Email Address, Phone Number, Photographic Identifiers, Employment Status, Occupation, Disease Status, Disease Signs and Symptoms, unique identifier, and Behavior Information that impacts Public Health. Social Security Numbers (SSN) are not allowed to be collected by EISWS. Data from this system is not shared with any other system(s). External users (survey respondents): No user credentials collected or required. Users navigate directly to survey with a system generated unique URL. Users do not authenticate in any way. Internal users are authenticated through Active Directory (AD). AD is a separate system with its own PIA.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	EISWS is a unique system that allows for the creation of a survey by a CDC user based on the need to conduct an epidemiologic investigation. The survey designer (CDC user) may choose to collect PII as part of their survey. All data (whether PII or not) will be stored inside the EISWS system. EISWS does not share any of this data with any other system. Data elements that can be collected in a survey include: Name, Date of Birth or Age, Sex, Mailing Address, Physical Address, Physical locations traveled, Email Address, Phone Number, Photographic Identifiers, Employment Status, Occupation, Disease Status, Disease Signs and Symptoms, and Behavior Information that impacts Public Health. A unique identifier will be used to keep track and link data to individuals. Social Security Numbers (SSN) are not allowed to be collected by EISWS. Data from this system is not shared with any other system(s). Survey respondents have the choice to not respond to specific questions or the survey itself. Examples of epidemiologic investigations that surveys can be created for: 1. Collecting baseline data regarding prevalence and incidence of infections on a specific disease in a given population. 2. Conduct community based evaluations of interventions. 3. Conduct surveys on attitudes and behaviors around specific public health initiatives. 4. Conduct surveys on Flu vaccine knowledge, attitudes and beliefs. 5. Conduct surveys about the level of knowledge and use of personal protective equipment in a hazardous workplace environment or among a particular occupation. External users (survey respondents): No user credentials collected or required. Users navigate directly to survey with a system generated unique URL. Users do not authenticate in any way. Internal users: Authenticated through Active Directory (AD). AD is a separate 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 ☒ 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 Physical locations traveled Disease Signs/Symptoms Occupation Behaviors Sex; Unique Identifier
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 assess exposure risks, monitor outcomes and interventions, monitor behaviors and their impact to public health interventions.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	Research and the assessment of policy and practice is the secondary use for the PII.
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, 42 U.S. Code § 300u
22	Are records on the system retrieved by one or more PII data elements?	○ Yes ◉ No

Save

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: 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.	None
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 ☐ 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

Save

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.	Epi Info Secure Web Survey employs the standard CDC Disclaimer and Use Warning that is used across CDC systems. It also states that users of the system *may* be asked to submit personally identifiable information (PII).	
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.	Individuals may opt-out of the collection and use of their PII by not participating or entering PII into the survey.	
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.	Should major changes ever occur to the system, CDC will not always have the capability to notify and obtain consent. The dependency is on the particular questions on the survey and its purpose (PII questions pertaining to contact information are not always asked). Surveys may not have any identifier other than a random number so there would be no way to know who filled out the form because submissions would be anonymous. If data use changes during or after the program collected data, and the survey collected contact information, then the program in question using Epi Info Secure Web Survey could contact the users directly to obtain consent for those changes. These terms are outlined in the system's Rules of Behavior (ROB) document.	
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.	The program contact that signed Epi Info's Rules of Behavior (ROB) document, is also the person who creates and publishes the surveys. The Rules of Behavior states that the program agrees to provide an email contact address within the survey for respondents to send questions or concerns. Thus, the program who designed and deployed the survey would be responsible for handling these concerns.	
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.	Epi Info Secure Web Survey system administrators require a CDC user to sign the Rules of Behavior in order to use Epi Info Secure Web Survey. Epi Info system administrators verbally go over the Rules of Behavior with the CDC user who signed it. The Rules of Behavior states that Epi Info Secure Web Survey system administrators will, at a minimum, annually review the surveys' PII for integrity, availability, accuracy and relevancy. They also have the right to review the PII collected at any time, if they suspect integrity, availability, accuracy, or relevancy has been compromised.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☐ Users ☒ Administrators ☐ Developers ☐ Contractors ☒ Others	 Administrators need to set up the data owner for the program in the system The program data owner of the form who has the key to publish the forms

Save

32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Epi Info program management assigns specific system administrators and developers, the authority to access, write, update, and maintain EISWS. Epi Info management also maintains a Web Survey Terms of Access and Use document that outlines how access is granted and outlines the publishing process.	
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.	Access for internal CDC system administrators is determined on a case-by-case basis by the EISWS program management. Both privileged and non-privileged users' access is governed by the principle of Least-Privilege, which restricts their access to the minimum functions and information essential to their job functions. The enforcement of the least-privilege model is controlled by the EISWS system; system administrators (privileged users) and non-privileged users are added to the EISWS security "Groups", and only members of those groups get access to the minimal data required to perform their duties. System administrators and developers (all of which are FTE) are provided access to the system based on need to know (i.e., Active Directory) and audit controls are in place to track their activity on the servers and within the consolidated database environment. These individuals are responsible for supporting, building, and maintaining the system itself and require full access to the entire application. There are system controls in place that limit a user's access to type, amount and categories of PII. Access to PII is first restricted by physical access. A CDC user must first be on the CDC network, they must have signed the Rules of Behavior (ROB), and have been granted access to the system by a system administrator and be provided an Organization Key in order to design a survey (that may or may not contain PII). The survey designer (CDC user) determines the amount of PII in their own surveys. Access to PII is further restricted through the process for publishing a survey. Once a CDC user has created a survey and would like to publish, they must use the Organization key to publish. At the time of publish, the CDC user receives two additional keys, a publisher key and a survey key. Only a person with all three keys can make changes to the survey, access the data collected in the survey, and perform analysis on it. The EISWS system is designed to only allow the survey creator/ designer to read/review/analyze the data that was collected from the survey they created. Physical access controls are in place as well as three encryption keys to ensure access to data is limited to the single individual who created and then published the survey. CDC users can not view or access surveys or survey responses of other CDC users' surveys that are also hosted by Epi Info Secure Web Survey.	

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.	All internal users of the system are required to complete the security and privacy awareness training at least annually.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	N/A
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.	Data is retained and disposed of in accordance with the CDC Records Control Schedule for EISWS: Per GRS 23.7 (), PII is stored for 2 years to allow CDC access to the information when requested. After two years, data is purged from the database.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Epi Info Secure Web Survey is a public facing application for administering surveys and and in internal-only Application Programming Interface (API) for accessing data: Administrative Controls – Programs agree to Rules of Behavior for PII data collection. Program will secure Office of Management and Budget / Institutional Review Board (OMB/ IRB) approval for the data being collected as per CDC requirement. Program will provide the form to Epi Info Secure Web Survey administrator to review the form for PII elements being collected prior to going live. Technical Controls – Technical controls are in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system. The application also utilizes the CDC's infrastructure firewalls, virus protection and intrusion detection systems for both the public facing site and intranet service. Physical Controls - Epi Info resides on client's CDC workstations that uses machine level encryption to encrypt data. EISWS database Servers are housed in secure CDC enterprise data centers that limit access to only authorized individuals part of Epi Info technical team. Physical controls include the use of human guards, identification badges, key cards, and Closed-Circuit Television (CCTV) in the server farm.
39	Identify the publicly-available URL:	http://www.cdc.gov/EpiInfo
40	Does the website have a posted privacy notice?	(•) Yes ( ) No
40a	Is the privacy policy available in a machine-readable format?	(•) Yes ( ) No
41	Does the website use web measurement and customization technology?	(•) Yes ( ) No

Save

		Technologies	Collects PII?
41a	Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)	☐ Web beacons	◯ Yes ◯ No
		☐ Web bugs	◯ Yes ◯ No
		☒ Session Cookies	◯ Yes ◯ No
		☐ Persistent Cookies	◯ Yes ◯ No
		Other...	◯ Yes ◯ No

42	Does the website have any information or pages directed at children under the age of thirteen?	◯ Yes ◉ No
43	Does the website contain links to non- federal government websites external to HHS?	◉ Yes ◯ No
43a	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	◉ Yes ◯ No

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.

	Reviewer Questions	Answer
1	Are the questions on the PIA answered correctly, accurately, and completely?	◯ Yes ◯ No
Reviewer Notes		
2	Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	◯ Yes ◯ No
Reviewer Notes		
3	Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	◯ Yes ◯ No
Reviewer Notes		
4	Does the PIA appropriately describe the PII quality and integrity of the data?	◯ Yes ◯ No
Reviewer Notes		
5	Is this a candidate for PII minimization?	◯ Yes ◯ No
Reviewer Notes		

Save

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

General Comments	

OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2020.06.15 08:34:14 -04'00'	HHS Senior Agency Official for Privacy	