Save

Privacy Impact Assessment Form

v 1.47.4

Status Draft Form Number F-67731 Form Date 8/31/2022 9:37:24 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-8654935-068130
2a	Name:	Anonymous Instance - Research Electronic Data Capture {REDCap} (AIREDC)
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 Business Steward POC Name Steve Racine POC Organization CDC\OID\NCEZID POC Email swr9@cdc.gov POC Phone 770.488.8292
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	Oct 14, 2022

Save

11	Describe the purpose of the system.	The Anonymous Instance - Research Electronic Data Capture (AIREDC) is an Internet web-based application for time-sensitive online survey data collection offered to CDC programs in support of epidemic or national public health events. The AIREDC application assists in managing Program specific time sensitive clinical intervention trials while collecting data on the efficacy of such trials. Application results will also assist epidemiological investigations in the field through the creation of dynamic data collection instruments. This system is housed within a FEDRamp approved Microsoft Azure facility within the CDC Office of the Chief Information Officer (OCIO) managed tenant.
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.)	AIREDC is a data collection tool offered to CDC programs to support public health research and public health emergency response. AIREDC projects and data requirements vary from public health research, laboratory research, emergency response, longitudinal studies, vaccine trial data, and other public health event. AIREDC can collect Non-Sensitive internal CDC Business Contact related data and is limited to name, CDC issued UserID, Branch/Division, and telephone number and from Public Health partner's Non-Sensitive Business data which is restricted to Point of Contact Name and business address, email and telephone number in support of epidemic and national health events. The exact nature, type and amount of Business Contact Personally Identifiable Information (PII) collected will vary from survey to survey. All AIREDC surveys are reviewed by a system Security Steward to ensure no sensitive PII or sensitive data is collected before being released for use other than Non-Sensitive Business contact data. For elevated functions, users are authenticated via CDC's Digital Support Office - Secure Access Management System (SAMS), including authorized CDC users. SAMS is a 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.	AIREDC is a COTS (REDCap) software develop for scientific research. The application was developed and is maintained by Vanderbilt University. Updates are managed and distributed by a consortium of partners that provide software support, development and communication. AIREDC is used for creating, fielding, and managing large or small data collection survey projects. Data collection projects encompass all facets of maintaining a research or public health response effort in the field. This includes data collection, management, analysis, and visualization purposes. AIREDC projects and data requirements vary from CDC's public health research, laboratory research, emergency response, longitudinal studies, vaccine trial data, and other public health event data. Under no circumstances will PII or sensitive information, other than business contact information (including name, E-mail address, phone number, and mailing address), be collected for clinical or epidemiological follow-up and intervention through this system in support of epidemic and national health events. For elevated functions that includes survey maintenance, data review, and the configuration of the application, the system users are authenticated via CDC's Digital Support Office - Secure Access Management System (SAMS), including authorized CDC users. SAMS is a 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 CDC User 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

Save

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?	To reach out to Business Point of Contact for follow up or clarification of public health survey information in support of epidemic and national health events.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	None
20	Describe the function of the SSN.	Not Applicable
20a	Cite the **legal authority** to use the SSN.	Not Applicable
21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	Public Health Service Act, Section 306(b) (42 U.S.C. 242k)
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 □ 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.	Not Applicable

Save

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.	AIREDC data projects may require governmental or non-governmental organizations contributing information to provide business contact information for accuracy or follow up analyses of epidemic or national public health events. Individual programs are responsible for ensuring processes are in place to notify business contact information will be collected for potential follow up. Specific point of contact name/email is optional whereas business telephone and address can be required. The AIREDC Security Steward reviews all surveys before release to ensure contact information is limited to business specific identity.
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.	AIREDC surveys are a one-time/time sensitive collection of data based on emerging public health events and no predefined process to opt out of collection of Business Contact Information. Surveys can provide an assessment of resources (supplies, personnel, knowledge) available and allow focus to change in response to needs. Individuals may choose not to participate with their specific business point of contact name and business email address for survey by submitting an alias name, i.e., Office Manager or Office Administrator and a generic business email account or disregard survey request.
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.	No process in place at application level. Individual data projects are responsible for the for their specific data collection and notification of significant changes to survey. AIREDC is a collection tool for a Program's survey. Significant or major changes to application would be transparent to survey participants. The Non-Sensitive Internal CDC and Partner Business Contact related survey data provides an assessment to epidemic and national health events.
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.	No process in place at application level. CDC relies upon programs to have appropriate processes and procedures in place to resolve individual concerns regarding the accuracy and handling of business contact information prior to survey submission.
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.	Not Applicable. AIREDC survey data is specific time sensitive data to assess epidemic and national health events. CDC relies upon programs to have appropriate processes and procedures in place to resolve individual concerns regarding the accuracy and handling of business contact information prior to survey submission.

Save

31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Program owners of survey data for review and analysis
		☒ Administrators	Application, User, Database, and Server Management.
		☐ Developers	
		☒ Contractors	Application, Database, and Server Management (restricted to CDC badged staff and direct contractors).
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The Business Steward limits access to the smallest possible number of people necessary to access PII data for conducting official responsibilities through specific Role-based	
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.	All CDC personnel are required to complete annual Security and Privacy Awareness Training.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Third party governmental and non-governmental data contributors receive role-based training regarding system access rules of behavior on a study by study 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.	Each program using AIREDC is responsible for applying its own existing records retention schedules and will vary across each program. Final reports and substantive reporting materials are maintained permanently (CDC RCS, B-321, 2&4). Routine reports are maintained until business use ceases or no longer needed as final reports are created (GRS 5.1 and 5.2). Other input/output records are disposed of when no longer needed (GRS 5.2). 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.	

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative controls: Controls include completion of training requirements; risk analyses performed annually; branch management reviewing access requests and granting minimal amount of access. Technical controls: Users are authenticated and data secured using operating system and server security, administered by the local system administrator. All data is encrypted at rest and in transits with access restricted to specific authorized users as required by HHS and CDC policy. All application user access to the AIREDC web application are authenticated via CDC's Digital Support Office-Secure Access Management System (SAMS), including authorized CDC users. Physical- Data is housed within the FEDRamp approved Microsoft Azure facility within the CDC OCIO managed tenant. The Azure data center's physical security begins at the perimeter layer. This layer includes a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures commensurate with the FEDRamp approval. All components of the AIREDC system reside in a CDC managed, FEDRamp approved Azure environment.
General Comments		Q10: System has moved to the OCIO Azure Operating environment from the on-premises environment. Change from Active Directory to CDC's Digital Support Office - Secure Access Management System (SAMS) as authentication mechanism.
OPDIV Senior Official for Privacy Signature		Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2022.09.26 12:54:47 -04'00'