Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-13599 | Form Date: 7/21/2022 9:44:14 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-6929567-366563
2a	Name:	Research Electronic Data Capture (REDCap)
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: Robert W Pinner POC Organization: CDC\OID\NCEZID POC Email: RPinner@cdc.gov POC Phone: 404.639.7710
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	Sep 16, 2022

Save

11	Describe the purpose of the system.	Research Electronic Data Capture (REDCap) is a data management platform for collection, analysis, and visualization of public health research and event data. This system exists in the CDC managed, FEDRamp approved
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.)	REDCap is a data collection tool offered to CDC programs in support of public health research and public health emergency response. REDCap projects and data requirements vary from public health research, laboratory research, emergency response, longitudinal studies, vaccine trial data, and other public health event data. For example, the data may include public health event studies that may collect information on symptoms and environmental exposures that may be linked to potential etiologic agents. In some circumstances, Personally Identifiable Information (PII) is collected for clinical or epidemiological follow-up and intervention. The exact nature, type, and amount of PII collected will vary from survey to survey but is limited to a subset of Name, Mother's Maiden Name, E-Mail Address Mailing, Phone Numbers, Medical Notes, Certificates, Education Records, Military Status, Foreign Activities, Date of Birth, Photographic Identifiers, Mailing Address, Medical Records Number, Legal Documents, Device Identifiers, or Employment Status per survey. All user access to the REDCap web application 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.	REDCap is an open source software develop for scientific research. The application was developed and maintained by Vanderbilt University. Updates are managed and distributed by a consortium of partners that provide software support, development and communication. At the CDC REDCap is used for creating, fielding, and managing large or small data collection 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. REDCap can also manage longitudinal studies that capture repeated measures on a study cohort. It also provides a comprehensive toolset to track study participants and their compliance/participation with the implemented research study protocol. REDCap projects and data requirements vary from public health research, laboratory research, emergency response, longitudinal studies, vaccine trial data, and other public health event data. For example, public health event studies might collect information on symptoms and environmental exposures that might be linked to potential etiologic agents. In some circumstances, PII is collected for clinical or epidemiological follow-up and intervention but is limited to a subset of Name, Mother's Maiden Name, E-Mail Address Mailing, Phone Numbers, Medical Notes, Certificates, Education Records, Military Status, Foreign Activities, Date of Birth, Photographic Identifiers, Mailing Address, Medical Records Number, Legal Documents, Device Identifiers, or Employment Status per survey. The exact nature, type and amount of PII collected will vary from survey to survey. All user access to the REDCap web application is 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

Save

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
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?	Most REDCap data projects do not contain PII. When PII is solicited, it is because the CDC 's Principal Investigator (PI) for each project leading that research project judges that PII may be important for that public health response, e.g. clinical trial follow-up after vaccine administration. The PI is responsible for Office of Management and Budget (OMB) clearance and communication about PII to respondents.
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. SSN are not collected or used.
20a	Cite the **legal authority** to use the SSN.	Not Applicable. SSN are not collected or used.
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)

Save

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.	If required, each individual project's program/Principle Investigator (PI) is responsible for obtaining the OMB information collection approval number. The PI is notified of and acknowledges this responsibility through the completion and acceptance of the REDCap Project Request Form. If OMB clearance is require for a project, the REDCap Project Request Form requires disclosure of the corresponding OMB information collection approval number and expiration date.
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.	For all REDCap data projects, CDC requires the governmental or non-governmental organizations (as defined in Q23 above) contributing the information to capture consent with the research or public health event by capturing a certified electronic signature for each participant in the research protocol or study. Each individual project's program/Principle Investigator (PI) is responsible for ensuring processes are in place to notify individuals that their personal information will be collected. The PI is notified of and acknowledges this responsibility through the completion and acceptance of the REDCap Project Request Form.
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.	For all REDCap data projects, CDC requires the governmental or non-governmental organizations (as defined in Q23 above) contributing the information to capture consent with the research or public health event by capturing a certified electronic signature for each participant in the research protocol or study. Each individual project's program/principle investigator (PI) is responsible for implementing methods for individuals to opt-out of the collection or use of their PII. The PI is notified of and acknowledges these responsibilities through the completion and acceptance of the REDCap Project Request Form.
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.	For all REDCap data projects, CDC requires the governmental or non-governmental organizations (as defined in Q23 above) contributing the information to capture consent with the research or public health event by capturing a certified electronic signature for each participant in the research protocol or study. Each individual project's program/Principle Investigator (PI) is responsible for implementing processes 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). The PI is notified of and acknowledges this responsibility through the completion and acceptance of the REDCap Project Request Form.
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.	Patient PII data are collected by governmental or non-governmental organizations (as defined in Q23 above) and are submitted to CDC in support of Public Health research or events. CDC has no direct involvement in the PII collection process or contact with the individuals. Each individual project's program/Principle Investigator (PI) is responsible for periodic reviews of the integrity, availability accuracy, and relevancy of PII collected. The PI is notified of and acknowledges this responsibility through the completion and acceptance of the REDCap Project Request Form. CDC relies upon those organizations to have appropriate processes and procedures in place to resolve individual concerns regarding the accuracy and handling of the PII prior to submission. However, upon request, the REDCap support team will help research system logs or otherwise assist the PIs with their investigations.
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.	Each individual project's program/Principle Investigator (PI) is responsible for periodic reviews of the integrity, availability accuracy, and relevancy of PII collected. The PI is notified of and acknowledges this responsibilities through the completion and acceptance of the REDCap Project Request Form.

Save

31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Data entry (open to all authorized users); Survey Design (restricted to CDC badged staff and contractor); and Data analysis (restricted to CDC
		☒ Administrators	Application, User, Database, and Server Management (restricted to CDC badged staff and contractors).
		☐ Developers	
		☒ Contractors	Direct contractors require access for data entry, Survey Design and Data analysis. Direct Contractors may act as Administrators as well.
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The Business Steward is limiting 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 REDCap is responsible for applying its own existing records retention schedules to PII data, and schedules will vary across programs. Specifically to REDCap, the records are maintained in accordance with General Records Schedule (GRS) and comply with CDC Records Control Schedule (RCS). In accordance with GRS 5.2, final reports are created to document programmatic decisions, policies, and other related issues and are maintained permanently (CDC RCS, B-321, 2&4). Input data of Non-electronic records manually data entered are maintained and disposed of when no longer needed. Other input/output records are disposed of when no longer needed: 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.	

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative controls: 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. PII data is encrypted at rest and in transits with access restricted to specific authorized users as required by HHS and CDC policy. All user access to the REDCap web application is 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 Office of the Chief Information Officer (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 REDCap 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.

OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2022.07.27 15:05:15 -04'00'