Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-69578 | Form Date: 5/5/2017 8:49:31 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-9247199-997552
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	Dec 8, 2014

Save

11	Describe the purpose of the system.	REDCap is a data management platform for collection, analysis, and visualization of public health research and event data. It provides users a tool set to manage clinical intervention trials in the field while collecting data on the efficacy of such trials. REDCap also assists epidemiological investigations in the field through creating dynamic data collection instruments.
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 projects and data requirements vary from public health research, laboratory research, emergency response, longitudinal studies, vaccine trial data, and other public health event data. As such, public health event studies might collect information on symptoms and environmental exposures that might be linked to potential etiologic agents. While most REDCap data projects do not contain PII, there are some circumstances when PII might be collected for clinical or epidemiological follow-up and intervention.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	REDCap is a data collection tool offered to CDC programs to support public health research and public health emergence response. At 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 tool set 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. While most REDCap data projects do not contain PIII, there are some circumstances when PII may be collected for clinical or epidemiological follow-up and intervention; the exact nature, type and amount of PII collected will vary from survey to survey.
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?	When PII is solicited for a research project, it is used for that particular public health response, e.g. clinical trial follow-up after vaccine administration.
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.	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 306(b) (42 U.S.C. 242k)
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.	There is no single information collection number available due to the unique and varied nature of REDCap data collection projects, an OMB information collection approval number is not always required. If required, however, each individual project's program/ principal investigator (PI) is responsible for obtaining an 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 required 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 source contributing the information to have obtained the participant's consent with the research or public health event by capturing a certified electronic signature from each participant in the research protocol or study beforehand.
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.	Most surveys do not request any PII. However when they do, CDC requires that respondents are also given the option of completing the survey without providing the requested PII. In these instances, while each individual project's program/ principal investigator (PI) is responsible for implementing methods for individuals to opt-out, any data gathered is then aggregated for entry into REDCap.
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 entity contributing the information to obtain participant consent with the research or public health event by capturing a certified electronic signature for each participant in the research protocol or study providing their PII. As a part of the official record, each project's program/principal investigator (PI) is responsible for implementing processes to ensure records belonging to the individual participants are maintained, transferred and destroyed according to either the general or project specific record retention requirements. If major changes to the disclosure and/or data uses of PII occur during this retention period, this consent documents will be used to notify and update the consenting individuals. As the CDC owner of the PII collected, each PI is responsible for both identifying major PII data use and disclosure changes and ensuring that the consenting individual is properly notified. The PI 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.	Individuals with concerns that their PII is inaccurate or may have been inappropriately obtained, used, or disclosed should first contact the contributing entity governmental or non-governmental organization) to which they initially disclosed the information. If unsatisfied with that collecting organization's response, the individual can contact CDC directly for assistance identifying the appropriate Principal Investigator (PI); as the CDC owner of the PII collected, each PI is responsible for working with individuals to resolve these types of concerns. The PI acknowledges this responsibility through the completion and acceptance of the REDCap Project Request Form.
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 these 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 ☒ Administrators: Data entry; Data analysis ☐ Developers: ☐ Contractors: ☐ Others:
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role-based access controls are used to determine which system users may access PII.
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 is used to allow those with access to PII to only access the minimum amount of information necessary to perform their job.
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 staff and contractors receive 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.	Final reports and substantive reporting materials are maintained permanently (CDC RCS, B-321, 2&4). Routine reports are maintained for five years (GRS 20.6). Other input/ output records are disposed of when no longer needed (GRS 20.2a.4, 20.2d, and 20.6). 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 include Federal, HHS, and CDC specific Privacy, Risk Assessment, and Incident Management Policies, annual system privacy impact assessments; and mandatory annual security & privacy awareness training. * Technical controls include application level role based access controls; standard baseline configurations for IT assets; encryption of PII at rest and in transit; and continuous monitoring of system resources identify vulnerabilities and ensure adherence to organizationally defined minimum security requirements. REDCap user access and authentication is controlled by CDC's Secure Access Management System. * Physical controls surrounding the system's data centers include gated campuses with 24-hour guards to enforce access restriction; key card access to campus buildings; and access control lists further limiting physical access to sensitive areas such as the data centers. All components of the RedCap system reside in CDC managed data center.

General Comments	

OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S DN: c=US, o=U.S. Government, ou=HHS, ou=CDC, ou=People, 0.9.2342.19200300.100.1.1=1001440343, cn=Beverly E. Walker -S Date: 2017.05.30 16:45:46 -04'00'