PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official. ***All entries must be Times New Roman, 12pt, and start on the next line.*** If you need further assistance, contact your LPO. A listing of the LPOs can be found here: https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: REDCap	**System Owner: Tracey Montilla**
Preparer: Tracey Montilla	**Office: ORD/CPHEA/PHITD/CRB**
Date: 8/25/21	**Phone: 919-966-7967**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☒	
Operation & Maintenance ☐ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

This is freeware software that is not opensource for electronic data capturing. It will help us manage our medical and study data better. The information collected is covered by SORN 34.

RedCap is a research electronic data capturing system. We will use this system for two purposes and the data collected will be partitioned accordingly:

(1.) To collect health information on study volunteers. This does contain PII. Volunteers are assigned a medical record number associated with their name and health information. We will use this as we have used our paper based medical records in the past. It will contain the same PII as listed in SORN 34. Only the medical station physicians and nurses have access to this information. This information will not be

shared with or linked to the partitioned study data section within RedCap.

(2.) To collect study data from research protocols. This study data does not contain PII. Any volunteer who participates in a study protocol is assigned a study number for the specific protocol they are participating in. That study number will be used to identify ALL study data for that participant. At no time do researchers have access to volunteer's personal health information. The study data will not be linked to the health records section partitioned in RedCap.

The data collected is covered under SORN 34. SORN 34 will be amended to reflect that health and medical data is not only kept in paper medical records but also in electronic record moving forward.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

U.S.C.6981; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9660; Clean Air Act, 42 U.S.C. 7403; Safe Drinking Water Act, 42 U.S.C. 300j-1; Federal Water Pollution Control Act, 33 U.S.C. 1254; Toxic Substances Control Act, 15 U.S.C. 2609; Federal Insecticide, Fungicide, and Rodenticide Act, 7 U.S.C. 136r.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

This system will be housed in the ORD GSS and will fall under the preview of that system ORD GSS ATO expires on June 30, 2023.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

The forms that collect demographic and health information from volunteers are attached to this file as pdf. Study forms that are created to collect/capture research data do not contain any PII data.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service

(PaaS, IaaS, SaaS, etc.) will the CSP provide?

No. It will be maintained in an ORD server that falls under ORD GSS.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

EPA/ORD/CPHEA human research protocols collect demographic and medical information on subjects who volunteer to participate in research. Names, addresses, email, telephone numbers of individual volunteers; individual vital statistics; medical histories; results of laboratory tests; results of participation in specific research studies; and related records pertinent to the human subject research program.

2.2 What are the sources of the information and how is the information collected for the system?

The subjects themselves are the source of demographic and medical histories. Information may be acquired through participation in research studies. Research study forms that are created to collect/capture research data do not contain any PII data.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No

2.4 Discuss how accuracy of the data is ensured.

The data provided by volunteers are assumed accurate.

2.5 <u>Privacy Impact Analysis</u>: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

<u>Privacy Risk:</u>

There is a minimal risk that the information provided by volunteers is inaccurate. Additionally, there is a minimal risk for a breach of confidentiality if an unauthorized user gains access to the

names, phone numbers and personnel health information of the volunteers.

Mitigation:

To help mitigate the risk of inaccurate information provided by volunteers, the submitted PII is reviewed by the volunteer and research nurse at the initial physical exam and annually provided the volunteer is an active participant in studies. The volunteer can inform the research nurse of any changes in their information at any time.

To help mitigate and prevent a breach of confidentiality, research study data for an individual will be identified by an assigned study number and not by their names. Only authorized users (medical staff) will have access to health information within REDCap. Designated REDCap administrators control access within the system and is determined by different roles and responsibilities of the research team. Administrators for the software participate in REDCap consortium network discussion. All Users receive training on REDCap.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

ORD GSS controls access and all controls in place. We have different levels of access and different levels of access are based on roles.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

In the ORD GSS Security Plan

3.3 Are there other components with assigned roles and responsibilities within the system?

Users have different roles/responsibilities and are assigned the appropriate level of access by designated REDCap administrators.

3.4 Who (internal and external parties) will have access to the

data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Only internal access. No contractor will have access to REDCap.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Records Schedule Number is 0566 and all information is retained indefinitely. The data is scientific in nature and need to be preserved incase we get asked any questions in the future about the data and the published results.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

Low risk of data getting into wrong hands during retention since data is kept indefinitely.

Mitigation:

We review the data routinely for data accountability.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No. Information is not shared externally.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

N/A

4.4 Does the agreement place limitations on re-dissemination?

N/A

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None. Information is not externally shared

Mitigation:

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy- based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

Access controls will be put in place to limit access to the system by designated user roles and assigned by REDCap administrators. Only the medical staff will have access to partition 1. Only specific study research team members have access to their individual study information in partition 2.

REDCap also has a user timestamp feature, as REDCap logs all user activity and builds audit trails for all projects within it. Any data imports or exports, changes to the data, user account changes, running of reports, pages viewed, etc. are logged by REDCap, indicating which user performed what action.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

None other than the annually required Information Security and Privacy Awareness Training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk of untimely audit.

Mitigation:

Logs are reviewed as appropriate.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

RedCap is an electronic data capturing system we will use for 2 purposes and will be partitioned accordingly:

(1.) To collect health information on study volunteers.

(2.) To collect study data from research protocols.

Acquired data is used for analyses in different research projects.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X__ No___. If yes, what identifier(s) will be used.

(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)

Health and demographic data stored in REDCap partition 1 will be retrieved by name whereas research study data stored in REDCap partition 2 will be retrieved by study number. There is no PII stored in REDCap partition 2.

The data collected is covered under SORN 34. SORN 34 will be amended to reflect that health and medical data is not only kept in paper medical records but also in electronic record moving forward.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

This system is currently being set up and will be evaluated periodically to make sure all appropriate controls and safeguards are in place.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There is a low risk associated to data misuse

Mitigation:

REDCap has user timestamp feature that indicates who modified the system and at what time it was modified. Privacy risk mitigation is a function of both the source systems and the ORD GSS security plan, which describes in detail the controls in place for the ORD GSS servers.

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

All volunteers sign a consent forms before providing us their PII.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

All volunteers sign a consent forms before providing us their PII for participation in research studies. The disclosure of their PII is voluntary.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Volunteers may not understand what or why their PII is collected, or what EPA is doing to protect their PII.

Mitigation:

All research volunteers participate in an informed consent process with investigators and designated research team members such as research study coordinator. Volunteers read, ask questions, and discuss the study protocol prior to providing consent for participation. This discussion includes collection of their PII and how their PII is protected under specific research protocols approved by EPA Human Subjects Research Review Official and appropriate Institutional Review Boards.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

There is a low risk that the volunteer might not be aware of the process to correct their PII.

Mitigation:

There is an appropriate process in place to update any changes in the PII of volunteers. Volunteers who want to continue participation in future studies must have a yearly physical exam and have an opportunity to update all their PII. Additionally, Volunteers can update their information at any time.