Save

Privacy Impact Assessment Form

v 1.21

Status | Form Number: 1A | Form Date: 02/02/21

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	TBD
2a	Name:	Assessment of Chemical Exposures (ACE) Investigations
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.	Planning
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: Surveillance Team Lead POC Name: Maureen Orr POC Organization: ATSDR POC Email: mco0@cdc.gov POC Phone: 404-567-3256
7	Is this a new or existing system?	◉ New ○ Existing
8	Does the system have Security Authorization (SA)?	○ Yes ◉ No
8b	Planned Date of Security Authorization	☒ Not Applicable

Save

8c	Briefly explain why security authorization is not required	The information collection will use multiple CDC authorized systems for data collection, analysis, and storage.
10	Describe in further detail any changes to the system that have occurred since the last PIA.	N/A
11	Describe the purpose of the system.	The ACE toolkit has data collection instruments, EPi Info databases and training materials that can be modified to perform a rapid epidemiological assessment. The ACE toolkit is used when an Epi AID is requested by state, regional, local, or tribal health departments. An Epi Aid involves ATSDR and other CDC staff including EIS officers. They are short intense investigations to help the requesting agency to respond to acute environmental incidents with multiple affected individuals.
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.)	ACE will collect, maintain, and share the following types of information: Participant's Identification (name, date of birth, mailing address, phone number, email address, social media accounts, social security number [SSN], driver's license number, state id number, and housing unit latitude and longitude) Participant's Emergency Contact (name, mailing address, email address, and phone number) Demographic (sex, education level, race, employment status, etc.) Exposure (location during exposure, decontamination, treatments, other people present, etc.) Medical (history, clinical tests and imaging results, etc.) Hospital Preparedness (surge, response, decontamination, lessons learned, etc.) Users will be authenticated by Active Directory (AD), an authorized CDC system.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	This data collection is to for rapid assessment after an acute environmental incident on behalf of the requesting (state/local or tribal) health agency. ATSDR will provide tools from its toolkit, technical expertise, laboratory and mapping expertise, and personnel support to requesting health agencies. Data collection will be conducted in the days or weeks following an acute environmental incident. The ACE investigation will collect, maintain, and share the following types of information: Participant's Identification, Participant's Emergency Contact, Demographic, Exposure, Medical, and Hospital Preparedness. Participant's identification, participant's emergency contact, demographic, and exposure information will be collected by our investigation staff in conjunction with and on behalf of the state or local health department trained volunteers. Participants will be members of the public who are age 18 or older. Information will be collected about individuals of all ages with a minor's data being provided by their parents or guardians. Hospital preparedness information is collected face to face by assessment staff from responding hospital staff. The participant's identification and emergency contact information is collected so that the states or health departments can contact affected individuals and follow up with them. The respondent Id is the link to the identifying information, that is the item that will be used for analysis. It can be used by the requesting agency to locate the individual, if necessary. Demographic information is collected to analyze the populations that were affected by the exposure and identify cohorts that may be followed and assessed for persistent health effects resulting from the exposure. Exposure and medical information is collected to characterize exposure and acute health effects of the affected community to inform health officials and the community. Hospital preparedness information is collected in order to assess the impact of the incidents on the health services used and share lessons learned for use in hospital, local, and state planning for environmental incidents. After a field investigation ends, ATSDR will transfer all data to the requesting health agency and delete all ATSDR copies of this data. A signed non-disclosure agreement between ATSDR and the requesting health agency will allow only deidentified data to be transferred to ATSDR. ATSDR will not retain the link between the respondent's direct identity (e.g., name, date of birth, address, phone number, email address) and the respondent ID number.
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 Other... Social media accounts Other... Other... Other...
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?	The primary purpose the PII is used is to avoid duplication in counting exposed people.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	The secondary uses of PII is to follow up with people and provide them with future services (medical services, testing, etc.).
20	Describe the function of the SSN.	In a large scale environmental disaster, many people may have similar names and DOB, the SSN will help to follow up with them and avoid duplication in counting. SSN is not required; other ID can be provided including drivers license or state ID. We will only collect the number of SSN digits necessary for the size of the incident. The SSN can also be used to help locate people to provide them information or services they may need as a result of the incident.
20a	Cite the **legal authority** to use the SSN.	ATSDR is authorized to collect SSN under the 'Comprehensive Environmental Response, Compensation, and Liability Act of 1980'' as amended by ''Superfund Amendments and Reauthorization Act of 1986'' (42 U.S.C. 9601, 9604); and the 'Resource Conservation and Recovery Act of 1976'' as amended in 1984 (42 U.S.C. 6901).

Save

21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	ATSDR is authorized under the 'Comprehensive Environmental Response, Compensation, and Liability Act of 1980'' as amended by ''Superfund Amendments and Reauthorization Act of 1986'' (42 U.S.C. 9601, 9604); and the 'Resource Conservation and Recovery Act of 1976'' as amended in 1984 (42 U.S.C. 6901).
22	Are records on the system retrieved by one or more PII data elements?	(•) Yes ( ) No
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: ATSDR SORN 09-19-0001. Records of Persons Exp 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.	OMB Control No: 0923-0051 (Expiration Date: 02/28/2021)
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 — The data including PII are given to th ☐ Private Sector

Save

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)).	Prior to initializing the ACE investigation the requesting agency and the ATSDR/CDC ACE lead will sign a Assessment of Chemical Exposures Technical Agreement which states that the data belongs to the requesting agency and that ATSDR and CDC will protect it while it is in their possession but will not retain it. The data will be given to the requesting health department at the investigation conclusion. and wiped form the CDC devices. Deidentified data may be provided to ATSDR by the requesting agency for analysis and publications. In this case a data sharing agreement, using the official CDC template will be executed. ATSDR will not share the data with any other entities. An internal ATSDR/CDC ACE Data Sharing Confidentiality Manual details these procedures.
24c	Describe the procedures for accounting for disclosures	We do not anticipate any disclosures of information by us. As we are collecting information on behalf of the requesting health departments and returning it to them, they will be responsible for accounting for any disclosures.
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.	The participant is given an informed consent to sign before providing their information. This information collection is governed by the Privacy Act which prohibits the disclosure of information from a system of records absent of the written consent of the subject individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records and sets forth various agency record-keeping requirements. Additionally, with people granted the right to review what was documented with their name, they are also able to find out if the "records have been disclosed".and are also given the rights to make correction
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.	The participant can decide not to participate in the investigation as explained by the informed consent. If we abstract all the medical records from a participating hospital we are doing this under the state health department's authority that does not require informed consent.
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.	The requesting health department maintains the data including the PII. They would have to obtain additional consent if needed.

Save

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 should contact the requesting health agency who maintains the PII. If the problem is with the data collection, the requesting health agency should contact the lead ATSDR investigator (varies by investigation type) to identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant. If an incident has occurred, the PI or data manager will report the potential incident to the Centers for Disease Control and Prevention (CDC) Security Incident Response Team and Privacy Officer. The data manager will serve as the point of contact to resolve 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.	ATSDR will only have access to PII for a limited time before it is transferred to the requesting organization and deleted by ATSDR. The health department who requested the investigation will be regulated by their own rules for periodic reviews of PII.
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users: PII will be entered into Epi Info, the ~~ATSDR/CDC staff collecting the data~~ ☐ Administrators: ☐ Developers: ☐ Contractors: ☐ Others:
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Only ATSDR or CDC staff who have read the internal ATSDR/ CDC ACE Data Sharing Confidentiality Manual and who are either collecting or entering data as part of the Epi Aid are allowed to see the 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 staff collecting data will only have access to the records they are collecting and not to the entire set of records. Records will be transferred to the main storage device every night and it will be stored under lock and key. At the end of the investigation, before leaving the field, all data will be stripped from the CDC/ ATSDR devices and will be further reimaged to make sure the PII is deleted permanently.
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.	ATSDR and CDC staff will all go through annual security awareness training. Additionally all staff will be required to read the internal ATSDR/CDC ACE Data Sharing Confidentiality Manual.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	There is instructions on data security in the ACE training manual and trainings. A training is conducted prior to the investigation's staff entering the field to collect data that covers data security and privacy .Additionally all staff will be required to read the internal ATSDR/CDC ACE Data Sharing Confidentiality Manual.

Save

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.	The PII is only kept until the data are entered, staff enter the data nightly as it is collected so that is is all entered before they leave the field, generally within 2 weeks. Then the data are transfered securely to the requesting agency and removed from the CDC/ATSDR devices permanently. If a data sharing agreement is signed and ATSDR/CDC obtains deideintified data for analysis and publications it will follow the destruction and retention of PII under Records Control Schedule CDC RG-0442, Scientific and Research Project Records, Minor Research Records which states that "the records should be maintained no longer than ten years after after the completion of the study, then delete/destroy. "
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	The PII in the system is secured using a layered approach with appropriate administrative, technical, and physical controls, being implemented. The administrative controls educate system users of their responsibility to protect PII and legally bind them to do so. These controls include signed rules of behavior , non-disclosure agreements, CDC privacy and security awareness training, and records management training. Records are maintained according to CDC record control policies and procedures. The technical controls, implemented by the system, act to either allow access to system PII data only to approved users or to make PII data unreadable outside of the system. These controls include encryption, authentication, firewalls, intrusion detection systems, and anti-malware systems. Data will be on entered on laptps or mobile devices and transferred to a main device at the end of each day of collection. It will then be put under lock and key. People entering data are instructed to lock there devices in a secure place when not in use and make sure their screens are not visible to others.

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		

Save

	Reviewer Questions	Answer
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		
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		

Save

General Comments			
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2021.02.03 12:25:50 -05'00'	HHS Senior Agency Official for Privacy	