Rules of Behavior for the Appropriate Use of Data Described in "Assessment of Chemical Exposures (ACE) Investigations"

Purpose:

The purpose of these rules of behavior (ROB) is to provide participants in this project with the rules that govern the appropriate use of the data described in the "Assessment of Chemical Exposures (ACE) Investigations" and to ensure that all parties using this data have agreed to these rules.

Description of Project: An Assessment of Chemical Exposures (ACE) investigation is requested as an Epi-AID by a health agency when there is an acute environmental incident that they need assistance to respond to. ATSDR/NCEH will provide a team of experts and EIS officers and use the ACE toolkit to respond immediately to assist the requesting agency. Potential activities include: to survey affected individuals, survey responding hospital staff, determine the extent of the exposure, and abstract medical chart data.

Applicable Datasets:

A signed non-disclosure agreement between ATSDR/NCEH and the requesting health agency will be required beforehand. Staff will all read the internal ACE Manual of Procedures before they sign this ACE Rules of Behavior. Data collection will span a few weeks after the request, after which time the data will be securely transmitted to the requesting agency and deleted from the encrypted CDC devices. A CDC data sharing agreement will be required to request data to be provided to ATSDR/NCEH for further analysis if needed. There are several surveys in the ACE toolkit (General, Child, Household, Hospital, Medical Chart, Epi CASE) that may be used to produce data for this investigation. All surveys may be shortened or omitted altogether depending on what the state requests. Mapping tools may be used to define the exposed area. In rare cases they may collect biologic samples from exposed individuals.

- Information will be collected about individuals of all ages with data on children under 13 data being provided by their parents or guardians.
- Personally Identifiable Information (PII) will potentially be collected and must be kept on CDC encrypted laptops and protected including:
    - Participant's Identification (respondent ID, 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)
    - Medical (history, clinical tests and imaging results, etc.)

The data stewards named below are responsible for protecting the confidentiality and integrity of the cohort data and any derived datasets.

Name	Title	Email	Phone Number
Maureen Orr	ACE project Lead	morr@cdc.gov	770-488-3806
Lead EIS officer TBD	Data Steward	xxx@cdc.gov	xxx-xxx-xxxx

The data stewards are also responsible for 1) determining who should have access to the data, 2) ensuring ROB's are signed by these individuals, 3) giving access to the data, 4) giving permissions to no more data than that required, 5) revoking access to the data when a user's role changes such that they no longer need access to the data or when a user leaves the investigation, and 6) using the data log to delete copies of the data when the data collection is completed.

The ROB's described below are specific for this project and supplement the following ROB's and policies:

1) CDC Implementation of the HHS Rules of Behavior for Use of HHS Information Technology Resources (2014)
2) HHS Rules of Behavior for Use of HHS Information Resources (2013)
3) CDC Protection of Information Resources Policy (2010)
4) Use of CDC Information Technology Resources (2014)

Users with access to the data in the "Assessment of Chemical Exposures (ACE) Investigations" agree that:

1) They will comply with all conditions set forth in any ***data use agreements for this project***.
2) They will follow procedures for securely transmitting, processing, and storing study data, as outlined in the ACE Manual of Procedures.
3) At the end of every day of data collection they will transmit the data to one main devie and data will be backed up on an encrypted common share \\cdc\locker\ATSDR_XXXX created with CDC's Multi-User Share Tool (MUST) http://itsotools.cdc.gov/must/. Only approved users will have access to the share.
4) They, approved users, must have a signed ROB, which will be stored in the shared drive, before they can access the data.
5) They shall only transfer data between CDC and the requesting health agency using CDC's Secure Access Management System (SAMS), e-Authentication Level 3, and approved FIPS 140-2 encryption. Other secure means, will be permitted if approved by ATSDR Information Systems Security Officer.
6) They will not download data to a non-encrypted CDC desktop or laptop. If another copy of the data is required, approved users will provide written notification on need, use, and duration of access of copy of data to the data stewards listed above. Approved users will create another copy in the encrypted common share. In addition, a log of all additional copies must be maintained in the common share.
7) If data must be downloaded for offline or desktop analysis, approved users will provide written notification on need, use, and duration of access of copy of data to the data stewards listed above. In addition, a log of all additional copies must be maintained in the common share. Furthermore, all data downloaded for offline or desktop analysis must be encrypted at the file level using the CDC managed and provided Symantec Encryption Desktop software.
8) All computers and laptops storing, processing, or transmitting PII data from this study and used by CDC FTE's and contractors (acting on CDC's behalf) must be provided by CDC, configured with CDC's standard image, and encrypted using FIPS 140-2 approved whole disk encryption.
9) They agree that all CDC systems processing the data must be authorized to operate by CDC and categorized as moderate or higher and approved to store, process or transmit personally identifiable information (PII). They acknowledge that they must obtain approval from the NCEH/ATSDR ISSO before any additional CDC systems are used to process, store or transmit this data.
10) They will not print out this data. If printing is absolutely necessary, then the printouts must be stored in locked cabinets when not in use and shredded when no longer needed.
11) They shall not transfer this data to external electronic media e.g. CD's, DVD's, thumb drives, portable hard drives, etc. without prior written approval from the NCEH/ATSDR ISSO.
12) They shall not transfer this data to a non-government, personally owned computing device.
13) They shall not transfer this data to non-CDC approved cloud based storage such as DropBox, One Drive, Google Drive, etc.
14) They shall not email this data to a personal, state, university, or any other non-CDC email address. Any transfer of this data outside of CDC must use CDC's SAMS or other system approved in writing by the NCEH/ATSDR ISSO.
15) They agree that only non-sensitive reports and statistical analyses may be transmitted via email. These emails cannot contain personally identifiable information (PII).
16) They agree that they are responsible for data compromise or breaches resulting from any copies they make of the data where the Rules of Behavior are not followed.
17) They agree to report any security breach immediately ***(within 1 hour)*** to both the NCEH/ATSDR ISSO (fgi5@cdc.gov, 770-488-6447) and the CDC Security Incident Response Team (CSIRT) (csirt@cdc.gov, 866-655-2245).
18) They agree to keep a copy of the signed ROB for their records and as a reference.

Name (printed): _____ Date: _____

CDC User ID: _____ Signature:_____