Security Procedures for Collecting, Storing, and Transferring Data in the Field Following a Chemical Release

Assessment of Chemical Exposures (ACE) Program

Internal Training Manual of Field Procedures for CDC/ATSDR Responders

Introduction

The purpose of this manual is to introduce CDC and ATSDR responders to standard security procedures for collecting, storing, and transferring data collected as a part of the Assessment of Chemical Exposures (ACE) program. This set of standard operating procedures (hereafter referred to as SOP) applies to CDC/ATSDR personnel (as defined below) who collect or use data as part of any ACE-related -activity which involves paper/hard copy records (HCR), biospecimens, or electronic records that contain personally identifiable information (PII). The SOP is intended to be a minimal standard for all ACE data collection activities involving PII. Therefore, any ACE investigation may adopt additional directives that are more stringent and adhere to the policies and guidelines of the agreement. These SOP are informed by the Privacy Act of 1974 (https://www.hhs.gov/foia/privacy/index.html) and the Health Information and Information Portability and Accountability Act (HIPAA; https://www.hhs.gov/hipaa/for-professionals/index.html.). These SOP do not address the retention schedule and destruction of records; for guidance on this issue please see the following CDC Records Management Policy as described in this link: http://intranet.cdc.gov/ocoo/strategic-business-initiatives-unit/records-management/index.html.

Confidentiality

All PII for ACE-related data collections containing names and other information identifying a single individual or a single institution and other data files, will be considered confidential materials and will be safeguarded to the greatest extent practicable under the Privacy Act of 1974. It is the professional and legal responsibility of each individual associated with each investigation to protect the right to confidentiality of the individuals and institutions in all ACE investigations, as defined by the Privacy Act of 1974 regarding personal data that is held by the Executive Branch of the U.S. Government, and other applicable federal regulations. Further, due to the scientific sensitivity and highly important intellectual property represented by the data, all personally identifiable data are considered confidential context of this SOP (see nhttps://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf). CDC/ATSDR responders are required at all times to maintain and protect the study data and confidential records that may come into their presence and under their control according to these SOPs and any additional guidelines as applicable.

Personally Identifiable Information (PII)

PII is any information that might serve to identify an individual. All precautions should be taken to protect the security of the eighteen identifying variables cited in HIPAA. The following list contains the eighteen HIPAA identifying variables:

1. Names;
2. All geographic subdivisions smaller than a State; including street address, city, county, precinct, zip code, and their equivalent geocodes (except for the initial three digits of a zip code if according to the current publicly available data from the Bureau of the Census the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000);
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers of any type (bank or other institutions, etc.);
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

Data Security and Confidentiality Policies and Procedures

Training—CDC/ATSDR responders authorized to access and use public health data are responsible for adhering to their programs' data security and confidentiality policies and procedures and should receive ongoing training on an annual basis on the appropriate collection, storage, use, and dissemination of data as defined by these policies.

1. PROGRAM POLICIES AND RESPONSIBILITIES

Creating policies and procedures.

- Designate a person or persons to act as the overall responsible party (ORP) for the security of collected data.
- Ensure that data security policies define the roles and access levels of all persons with authorized access to confidential public health data and the procedures for accessing data securely.
- Ensure that data security policies require ongoing reviews of evolving technologies and include a computer back-up or disaster recovery plan. The National Institute of Standards and Technology Special Publication 800-34, Contingency Planning Guide for Federal Information Systems contains guidance on contingency planning for IT resources and is available at: http://csrc.nist.gov/publications/PubsSPs.html . [25]
- Ensure that any breach of data security protocol, regardless of whether personal information was released, is reported to the ORP and investigated immediately. Any breach that results in the release of PII to unauthorized persons should be reported to the ORP, to CDC, and, if warranted to law enforcement agencies.
- Ensure that staff members with access to PII attend data security and confidentiality training annually.
- Require all ACE responders to sign a confidentiality agreement before being given access to identifiable information;
- Ensure that all persons who have authorized access to confidential public health data take responsibility for 1) implementing the program's data security policies and procedures, 2) protecting the security of any device in their possession on which PII are stored, and 3) reporting suspected security breaches.

2. DATA COLLECTION AND USE

- Clearly specify the purpose for which the data will be collected.
- Collect and use the minimum information needed to conduct specified public health activities and achieve the stated public health purpose.
- Collect personally identifiable data only when necessary; use nonidentifiable data whenever possible.
- Use only CDC encrypted devices to collect data.
- Make sure that data are transferred to one main device either by encrypted media or email daily, removing it from the other devices.
- Upload a copy of the data to a secure CDC directory every night so that there is a copy in case the device fails.
- At the end of the investigation, before leaving the field, transfer all data to the requesting health agency on encrypted media or email. Remove the data from all devices/directory.
- When returning to CDC/ATSDR put in a ticket to ITSO to have the devices reimaged to remove all traces of data.

DATA-SHARING PLANS—**If you are requested to complete additional analysis after leaving the field, a data sharing agreement will be necessary. Using the CDC data sharing template** as a starting point for discussions about data sharing between or among public health programs. A data-sharing plan should include:

- Intent and scope of data sharing
- Potential benefits (including projected efficiencies) and risks of sharing, benefits and risks of not sharing, and methods to monitor these benefits and risks
- Methods that will be used to share data and roles and responsibilities of staff involved
- Minimum data elements needed to achieve the objective(s), including need for PII
- Steps that will be taken to ensure the confidentiality and security of shared data
- Provisions for physical and electronic security
- How shared data will be used, analyzed, published, released, and retained/destroyed
- Confidentiality agreements

- Knowledge and training requirements including annual training for staff who have access to PII and non-PII data.

Restrictions on Use of Information

1. Personal identifying information collected or retrieved by CDC/ATSDR personnel following a chemical release will be used only for the purposes of carrying out program activities and shall not be divulged or made known in any manner to non-program personnel unless prior written approval from the data collection participant is received.
2. Program personnel are responsible for protecting all confidential records from visual observation, from theft, and from accidental loss or misplacement as required by law.
3. Any materials containing personal identifiers that must be sent by authorized program personnel must be sent via first class certified-return receipt mail or commercial carrier service in a sealed envelope stamped “CONFIDENTIAL” on the front.
4. Program personnel are not to divulge any personal identifying information about project participants to anyone other than authorized program personnel on a “need to know” basis appropriate to conduct official business. In general conversation outside the workplace, neither the identifying information nor specific details about the PII data collected should be discussed in any detail. Breach of confidentiality due to program personnel knowingly and willfully disclosing confidential information may result in removal from project activities and administrative, as well as legal, actions. If a breach of confidentiality is due to unintentional, but careless, behavior and/or not following policies to maintain confidentiality of data, the behavior will result in, at a minimum, a temporary removal from accessing confidential information, and specific sanctions may apply such as Subsection 5 of the Privacy Act of 1974 (see https://www.justice.gov/opcl/criminal-penalties).
5. When not in use by authorized program personnel, all HCR containing confidential data will be stored in locked containers, locked file cabinets, or locked rooms. Access to locked storage areas will be limited to authorized program personnel. This procedure will also apply to all physical media containing confidential data. Program personnel working with any confidential materials will have access only to the materials that they

are currently processing. When confidential records are in use, they must be kept out of sight of persons not authorized to work with these records.

6. Except as needed for operational purposes, copies (including any other hard or electronic media, e.g., photocopies or electronic scans) of confidential records are not to be made. If photocopies are necessary, care should be taken that all copies and originals are recovered from the copy machines and work areas. Whenever practicable, copy machines should be the type that do not retain hard drive copies of documents, or that provide the capability to delete copies from the hard drive. All confidential paper records will be destroyed as soon as the field investigation terminated. If electronic scans are necessary, care should be taken to adhere to all electronic data security requirements (see the main website of Office of Chief Information Officer (OCIO) for more information http://intranet.cdc.gov/ocio/information-systems-security/privacy-information-security/description-requirements/index.html)

7. As a general rule, unless a SECURE FAX machine is available, faxing any records containing PII should be avoided. If PII must be faxed, the following steps should be taken:
    i. **Sending fax:**
        1. Verify recipient's fax number prior to sending PII.
        2. Ensure someone authorized to receive the PII is there to receive the fax.
        3. Use a fax transmittal sheet. Consider adding a Confidentiality Statement to the fax cover sheet.
    ii. **Receiving a fax:**
        1. Quickly retrieve transmitted faxes.
        2. Secure faxes that have not been retrieved.
        3. If an expected fax has not been received, follow-up to ensure that the sender has the correct fax number.

8. Unless specifically instructed otherwise (for a particular project approved by the program's Security Steward) program personnel will not be allowed to abstract, collect, or process any data from a respondent whom they know personally.

Data sharing with Other Study Partners

Individually identified data on individuals or establishments (sources, diagnosticians, etc.) derived will only be shared across project sites or with non-project personnel upon specific approval of the project's Security Steward or designee. Any use or analysis of project data must be in line with the original purpose for which the data have been collected, which is a public health response, or re-review by CDC and local IRB(s) might be necessary. The CDC

Confidentiality Officer should be consulted if there are requests that present unusual circumstances or appear to be outside intended boundaries for use (such as FOIA).