

## XIV. DATA SECURITY AND CONFIDENTIALITY

### **MODULE OUTLINE**

1. Standards of Public Health Practice
  2. Program Policies and Responsibilities
  3. Data Collection and Use
  4. Data Sharing and Release
  5. Physical Security
  6. Electronic Data Security
  7. Ten Guiding Principles for Data Collection, Storage, Sharing and Use to Ensure Security and Confidentiality
- 

### **1. STANDARDS OF PUBLIC HEALTH PRACTICE**

XIV-1. Each regional/metro TB program adheres to the TB data security guidance in accordance with the TTBEF Manual.

**NOTE:** The data security guidelines below are taken from the following document: Centers for Disease Control and Prevention. Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action. Atlanta (GA): U.S. Department of Health and Human Services, Centers for Disease Control and Prevention; 2011.

This document can be accessed at:

<http://www.cdc.gov/nchhstp/programintegration/docs/PCSIDataSecurityGuidelines.pdf>

Each regional/metro TB program adheres to TB data security guidance in accordance with this manual (**Standard of Public Health Practice XIV-1**).

### **2. PROGRAM POLICIES AND RESPONSIBILITIES**

- Develop written policies and procedures on data security and confidentiality.
  - Review policies and procedures at least annually and revise them as needed.
  - Ensure the review by and accessibility to all staff members having authorized access to confidential individual-level data.
- Designate a person(s) to act as the overall responsible party (ORP) at the regional and county level for the security of public health data that a program collects or maintains, and ensure that the ORP is named in any policy documents related to data security.
- 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 receive ongoing reviews of evolving technologies and include a computer back-up or disaster recovery plan.
- 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 personally identifiable information (PII) to unauthorized persons should be reported to the county and regional ORP, to CDC, and, if warranted, to law enforcement agencies.
- Ensure that staff members with access to identifiable public health data attend data security and confidentiality training annually.
- Require all newly hired staff members to sign a confidentiality agreement before being given access to identifiable information.
  - Require all staff members to re-sign their confidentiality agreements annually.
- Ensure that all persons who have authorized access to confidential public health data take responsibility for:
  - Implementing the program’s data security policies and procedures, and
  - Protecting the security of any device in their possession on which PII are stored, and
  - Reporting suspected security breaches.
- Certify annually that all data security standards have been met.

### **3. 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 non-identifiable data whenever possible.
- Ensure that data that are collected and/or used for public health research are done in accordance with stipulations in Common Rule, Title 45, Part 46 of the Code of Federal Regulations, which includes obtaining both institutional review board (IRB) approval for any proposed federally funded research and informed consent of individuals directly contacted for further participation.
  - These stipulations can be found at:  
<http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html>

### **4. DATA SHARING AND RELEASE**

- Limit sharing of confidential or identifiable information to those with a justifiable public health need.
  - Ensure that any data-sharing restrictions do not compromise or impede public health program or disease surveillance activities and that the ORP or other appropriate official has approved this access.
- Assess the risks and benefits of sharing identifiable data for other than their originally stated purpose or for purposes not covered by existing policies.

- Ensure that any public health program with which personally identifiable public health data are shared has data security standards equivalent to those in this document.
- Ensure that public health information is released only for purposes related to public health, except where required by law.
- Establish procedures, including assessment of risks and benefits, for determining whether to grant requests for aggregate data not covered by existing data-release policies.
- Disseminate non-identifiable summary data to stakeholders as soon as possible after data are collected.
- Assess data quality before disseminating data.
- Ensure that data-release policies define purposes for which the data can be used and provisions to prevent public access to raw data or data tables that could contain indirectly identifying information.

## **5. PHYSICAL SECURITY**

- To the extent possible, ensure that persons working with hard copies of documents containing confidential, identifiable information do so in a secure, locked area.
- Ensure that documents containing confidential information are shredded with cross-cutting shredders before disposal.
- Ensure that data-security policies and procedures address handling of paper copies, incoming and outgoing mail, long-term paper storage, and data retention.
- The amount of confidential information in all such correspondence should be kept to a minimum and destroyed when no longer needed.
- Limit access to secure areas that contain confidential public health data to authorized persons, and establish procedures to control access to secure areas by non-authorized persons.
- Ensure that program personnel working with documents containing personally identifiable information in the field:
  - Return the documents to a secure area by close of business,
  - Obtain Prior Authorization from the program manager for not doing so, or
  - Follow approved procedures for handling such documents.
- Ensure that documents with line lists or supporting notes contain the minimum amount of potentially identifiable information necessary and, if possible, that any potentially identifiable data are coded to prevent inadvertent release of PII.

## **6. ELECTRONIC DATA SECURITY**

- Ensure that analysis data sets that can be accessed from outside the secure area are stored with protective software (i.e., software that controls data storage, removal, and use), and verify removal of all identifiers.
- Ensure that any electronic transfer of data is approved by the ORP and subject to access controls, and that identifiable data are encrypted or in a password protected document before being transferred.

- Before transferring electronic data containing PII, ensure that the data have been encrypted with use of an encryption package that meets Advanced Encryption Standard (AES) criteria and that the data transfer has been approved by the appropriate program official or ORP.
- The AES criteria can be found at: <http://csrc.nist.gov/publications/nistbul/itl97-02.txt>
  - No electronic data containing identifying information should be transferred without being encrypted.
- Use encryption software that meets federal AES standards to encrypt data with PII on all laptops and other portable devices that receive or store public health data with personal identifiers.
- Ensure that data policies include procedures for handling incoming and outgoing facsimile transmissions.
  - Minimize inclusion of PII in fax transmissions, and destroy hard copies and sanitize hard drives when no longer needed.

**7. TEN GUIDING PRINCIPLES FOR DATA COLLECTION, STORAGE, SHARING, AND USE TO ENSURE SECURITY AND CONFIDENTIALITY**

Table XIV-1 outlines the ten guiding principles for data collection, storage, sharing, and use to ensure security and confidentiality:

**Table XIV-1: Ten Guiding Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality**

1.	Public health data should be acquired, used, disclosed, and stored for legitimate public health purposes.
2.	Programs should collect the minimum amount of personally identifiable information necessary to conduct public health activities.
3.	Programs should have strong policies to protect the privacy and security of personally identifiable data.
4.	Data collection and use policies should reflect respect for the rights of individuals and community groups and minimize undue burden.
5.	Programs should have policies and procedures to ensure the quality of any data they collect or use.
6.	Programs have the obligation to use and disseminate summary data to relevant stakeholders in a timely manner.
7.	Programs should share data for legitimate public health purposes and may establish data-use agreements to facilitate sharing data in a timely manner.
8.	Public health data should be maintained in a secure environment and transmitted through secure methods.
9.	Minimize the number of persons and entities granted access to identifiable data.
10.	Program officials should be active, responsible stewards of public health data.

Reference:

1. Lee, LM, Gostin, LO. Ethical collection, storage, and use of public health data: a proposal for national privacy protection. JAMA 2009; 302:82-84 (adapted).