**Data Security and Confidentiality Tool - 1**

**Data Security and Confidentiality Guidelines for
HIV, Viral Hepatitis, STD, and TB Programs**

 ***Standards to Facilitate Data Sharing and Use of Surveillance Data for Public Health Action***

1.0 PROGRAM POLICIES AND RESPONSIBILITIES

1.1 Develop written policies and procedures on data security and confidentiality; review policies and procedures at least annually; revise them as needed; and ensure their review by and accessibility to all staff members having authorized access to confidential individual-level data.

1.2 Designate a person or persons to act as the overall responsible party (ORP) for the security of public health data your program collects or maintains, and ensure that the ORP is named in any policy documents related to data security.

1.3 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.

1.4 Ensure that data security policies require ongoing reviews of evolving technologies and include a computer back-up or disaster recovery plan.

1.5 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 ORP, to CDC, and, if warranted to law enforcement agencies.

1.6 Ensure that staff members with access to identifiable public health data attend data security and confidentiality training annually.

1.7 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.

1.8 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.

1.9 Certify annually that all data security standards have been met.

2.0 DATA COLLECTION AND USE

2.1 Clearly specify the purpose for which the data will be collected.

2.2 Collect and use the minimum information needed to conduct specified public health activities and achieve the stated public health purpose.

2.3 Collect personally identifiable data only when necessary; use nonidentifiable data whenever possible.

2.4 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.

3.0 DATA SHARING AND RELEASE

3.1 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.

3.2 Assess the risks and benefits of sharing identifiable data for other than their originally stated purpose or for purposes not covered by existing policies.

3.3 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.

3.4 Ensure that public health information is released only for purposes related to public health, except where required by law.

3.5 Establish procedures, including assessment of risks and benefits, for determining whether to grant requests for aggregate data not covered by existing data-release policies.

3.6  Disseminate nonidentifiable summary data to stakeholders as soon as possible after data are collected.

3.7 Assess data quality before disseminating data.

3.8 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.

4.0 PHYSICAL SECURITY

4.1 To the extent possible, ensure that persons working with hard copies of documents containing confidential, identifiable information do so in a secure, locked area.

4.2 Ensure that documents containing confidential information are shredded with crosscutting shredders before disposal.

4.3 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.

4.4 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.

4.5 Ensure that program personnel working with documents containing PII in the field 1) return the documents to a secure area by close of business, 2) obtain prior approval from the program manager for not doing so, or 3) follow approved procedures for handling such documents.

4.6 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.

5.0 ELECTRONIC DATA SECURITY

5.1 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 personal identifiers.

5.2 Ensure that any electronic transfer of data is approved by the ORP and subject to access controls, and that identifiable data are encrypted before being transferred.

5.3 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. No electronic data containing identifying information should be transferred without being encrypted.

5.4 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.

5.5 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.