

# Appendix B.

## Checklists for Assessment of Data Security and Confidentiality Protections

### INITIAL ASSESSMENT

This checklist can be used to guide the initial assessment of a program's compliance with the Standards for Data Security and Confidentiality. This will be particularly useful for state and local public health programs that currently lack data security and confidentiality policies and procedures.

As indicated previously in this document, the initial assessment should be conducted by a team led by the ORP(s). The team should include:

- Program managers, directors, or equivalent leaders from participating programs
- Other representatives of participating programs
- Staff members with technical expertise in data security
- IT staff

The initial assessment should include the following steps:

- Identify key individuals and designate an ORP
- Review current security-related materials (e.g., written policies and procedures)
- Review relevant state and local laws that might affect data security and confidentiality policies
- Identify any policies or procedures that are either barriers to information sharing or sources of data security weaknesses
- Consult standard operating procedures (SOPs) from other programs that might be useful sources of ideas or suggestions for procedural changes
- Review any history of data security breaches or near-breaches, and associated lessons learned
- Assess physical security and define the secure area
- Assess electronic security protections and methods of data transfer and storage
- Assess factors related to security of information in the field, as appropriate
- Assess training needs

## CONDUCTING AN INITIAL ASSESSMENT: STEPS AND GUIDING QUESTIONS

<p><b>Identify key individuals and designate an ORP</b></p>	<p>Have key individuals, including program managers, directors, persons responsible for information and system security, and appropriate technical staff members, been identified?</p> <p>Has an ORP(s) with ultimate decision-making authority and responsibility for reconciling differences in policies and procedures across programs been identified?</p>
<p><b>Review current policies and gather resources</b></p>	<p>Have relevant policies, data-sharing agreements, and standard operating procedures been compiled and reviewed?</p> <p>Have relevant laws, rules, and regulations been considered?</p>
<p><b>Identify weaknesses and barriers</b></p>	<p>Have areas of weakness and specific topics that need additional clarification been identified?</p> <p>Have barriers to data sharing been identified?</p> <p>Have potential solutions to these barriers, including possible policy revisions, been noted?</p>
<p><b>Assess physical security and define the secure area</b></p>	<p>What is the work-space configuration?</p> <p>What is the path of public health data from collection and entry into the program's physical space through data entry and storage?</p> <p>What happens to case report forms received from providers? How are case report forms completed by health department staff handled? Is information obtained by phone or other electronic format? If so, how are hard copies or electronic media physically secured? Are electronic devices used, such as PDAs or laptops? If so, how are these physically secured?</p> <p>How is the area that houses identifiable data secured?</p> <p>Who has access to the physical space, who needs access, and for what purpose?</p>
<p><b>Assess electronic security, protections, and methods of data transfer and storage</b></p>	<p>Who or what roles need access to identifiable data? At what stage is their access required?</p> <p>Who needs access to electronic databases with identifiable data?</p> <p>Who needs access only to de-identified or analysis data sets?</p> <p>Who teleworks and what level of access do they need? Are electronic protections in place for remote access?</p> <p>Which individuals must take identifiable information in the field or outside of the secure physical area or health department? How is that information brought back into the office and what happens when it arrives?</p> <p>Does field work involve information on paper or electronic data on laptops or other storage devices?</p> <p>What electronic protections are in place during data transfer? Is encryption used? If so, when are data encrypted? Are data encrypted while at rest?</p> <p>Are data ever transported between locations across secured boundaries such as a secure data network (SDN), virtual private network, or Secure File Transfer Protocol (SFTP)?</p>
<p><b>Assess training needs</b></p>	<p>Do all programs involved have specific security and confidentiality training? How often is it conducted and who does it?</p> <p>What additional training will be required if policies are modified?</p> <p>Do other types of employees need to be trained (e.g. mail room staff, maintenance and cleaning staff, security staff, IT staff [in-house and contracted services])?</p> <p>How often are training materials updated?</p>

## Periodic Assessment Checklist

This checklist can be used to guide the periodic assessment of a program's compliance with the Standards for Data Security and Confidentiality.

**For the answer to be "yes" to a question with multiple parts, all boxes must be checked. For each "No" response, provide additional information describing how the program intends to achieve compliance with that standard.**

Name of Program being assessed

Name of person assessing the program

### 1.0 PROGRAM POLICIES AND RESPONSIBILITIES

#### STANDARD 1.1

In your program, how are staff members who are authorized to access HIV/VH/STD/TB information or data made aware of their data confidentiality and security responsibilities?

---

---

*Are the following points addressed in your policies and agreements?*

- 
- Yes  No Are staff provided training on security policies and procedures and where to find resources?
- 
- Yes  No Does the program have written data security and confidentiality policies and procedures?
- 
- Yes  No Are written policies and procedures reviewed at least annually and revised as needed?
- 
- Yes  No Are data security policies readily accessible to all staff members who have access to confidential, individual-level data?  
Where are the policies located? \_\_\_\_\_
-

---

**STANDARD 1.2**

---

- Yes  No In your program, is there a policy that assigns responsibilities and designates an ORP for the security of the data that is stored in various data systems?
- 
- Yes  No Does the ORP have sufficient authority to make modifications to policies and procedures and ensure that the standards are met?
- 

---

**STANDARD 1.3**

---

- Yes  No Does your program have a policy that defines the roles and access level for all persons with authorized access?
- 
- Yes  No Does your program have a policy that describes which standard procedures or methods will be used when accessing HIV/VH/STD/TB information or other personally identifiable data?
- 

---

**STANDARD 1.4**

---

- Yes  No Does the program have a written policy that describes the methods for ongoing review of technological aspects of security practices to ensure that data remain secure in light of evolving technologies?
- 

---

**STANDARD 1.5**

---

- Yes  No Are written procedures in place to respond to breaches in procedures and breaches in confidentiality?  
Where are those procedures stored? \_\_\_\_\_
- 
- Yes  No Is the chain of communication and notification of appropriate individuals outlined in the data policy?
- 
- Yes  No Are all breaches of protocol or procedures, regardless of whether personal information was released, investigated immediately to determine causes and implement remedies?
- 
- Yes  No Are all breaches of confidentiality (i.e., a security infraction that results in the release of private information with or without harm to one or more persons) reported immediately to the ORP?
- 
- Yes  No Do procedures include a mechanism for consulting with appropriate legal counsel to determine whether a breach warrants a report to law enforcement agencies?
- 
- Yes  No If warranted, are law enforcement agencies contacted when a breach occurs?
-

### STANDARD 1.6

- Yes  No Are staff trained on the program's definitions of breaches in procedures and breaches in confidentiality?
- Yes  No Are staff trained on ways to protect keys, use passwords, and codes that would allow access to confidential information or data?
- Yes  No Are staff trained on policies and procedures that describe how staff can protect program software from computer viruses and computer hardware from damage due to extreme heat or cold?
- Yes  No Have all persons authorized to access individual-level information been trained on the organization's information security policies and procedures?
- Yes  No Is every staff member, information technology (IT) staff member, and contractor who may need access to individual-level information or data required to attend security training annually?
- Yes  No Is the date of the training or test documented in the employee's personnel file?

### STANDARD 1.7

- Yes  No Do all authorized staff members in your program sign a confidentiality agreement annually?
- Yes  No Do all newly hired staff members sign a confidentiality agreement before they are given authorization to access individual-level information and data?

### STANDARD 1.8

- Yes  No Do policies state that staff are personally responsible for protecting their own computer workstation, laptop computer, or other devices associated with confidential public health information or data?
- Yes  No Are staff trained on ways to protect keys, use passwords, and codes that would allow access to confidential information or data?

### STANDARD 1.9

- Yes  No Does your program certify annually that all program standards are met?

## 2.0 DATA COLLECTION AND USE

### STANDARD 2.1

---

Yes  No

When public health data are shared or used, are the intended public health purposes and limits of how the data will be used adequately described?

---

### STANDARD 2.2

---

Yes  No

When data are collected or shared, do they contain only the minimum information necessary to achieve the stated public health purpose?

---

### STANDARD 2.3

---

Yes  No

Does your program explore alternatives to using identifiable data before sharing data, such as using anonymized or coded data?

What alternatives are currently in use in your program? \_\_\_\_\_  
\_\_\_\_\_

---

### STANDARD 2.4

---

Yes  No

Does your program have procedures in place to determine whether a proposed use of identifiable public health data constitutes research requiring IRB review?

---

## 3.0 DATA SHARING AND RELEASE

### STANDARD 3.1

---

Yes  No

In your program, is access to HIV/VH/STD/TB information and data for any purposes unrelated to public health (e.g., litigation, discovery, or court order) only granted to the extent required by law?

What non-public health use of the data are required or allowed by law?  
\_\_\_\_\_

---

**STANDARD 3.2**

---

When a proposed sharing of identifiable data is not covered by existing policies, does your program assess risks and benefits before making a decision to share data?

Yes  No

How are these risks assessed? \_\_\_\_\_  
\_\_\_\_\_

---

**STANDARD 3.3**

---

When sharing personally identifiable HIV/VH/STD/TB information and/or data with other public health programs (i.e., those programs outside the primary program responsible for collecting and storing the data), is access to this information and/or data limited to those for whom the ORP:

Yes  No

- has weighed the benefits and risks of allowing access; and
  - can verify that the level of security established is equivalent to these standards?
- 

**STANDARD 3.4**

---

Is access to confidential HIV/VH/STD/TB information and data by personnel outside the HIV/VH/STD/TB programs:

Yes  No

- limited to those authorized based on an expressed and justifiable public health need?; and
  - arranged in a manner that does not compromise or impede public health activities?; and
  - carefully managed so as to not affect the public perception of confidentiality of the public health data collection activity and approved by the ORP?
- 

Before allowing access to any HIV/VH/STD/TB data or information containing names for research or other purposes (e.g., for other than routine prevention program purposes), does your program require that the requester:

Yes  No

- demonstrate need for the names?; and
  - obtain institutional review board (IRB) approval (if it has been determined to be necessary)?; and
  - sign a confidentiality agreement?
-

**STANDARD 3.5**

---

Yes  No

Does your program have written procedures to review data releases that are not covered under the standing data release policy?

---

If not, does your program have unwritten policy to review data releases that are not covered under the standing data release policy?

Yes  No

Describe briefly those procedures or policies: \_\_\_\_\_  
\_\_\_\_\_

---

**STANDARD 3.6**

---

Yes  No

Does your program routinely distribute nonidentifiable summary data to stakeholders?

---

**STANDARD 3.7**

---

Yes  No

Does your program assess data for quality before disseminated?

---

**STANDARD 3.8**

---

Yes  No

Does the program have a data-release policy that defines access to, and use of, individual-level information?

---

Yes  No

Does the data-release policy incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying information?

---

## 4.0 PHYSICAL SECURITY

### STANDARD 4.1

---

Are workspaces and paper copies for persons working with confidential, individual-level information located within a secure, locked area?

Yes  No

- Are sensitive documents stored in cabinets?
  - Are the cabinets locked?
  - Are cabinets located in an area to which there is no access by unauthorized employees?
  - Are cabinets located in an area to which there is no public access?
- 

### STANDARD 4.2

---

Yes  No

Do program staff members shred documents containing confidential information with a cross-cutting shredder before disposing of them?

---

### STANDARD 4.3

---

Yes  No

Does your program have a written policy that outlines procedures for handling paper documents which could contain confidential information that are mailed to, or from, the program?

---

Yes  No

Do staff members in your program ensure that the amount and sensitivity of information contained in any piece of correspondence remains minimal?

---

### STANDARD 4.4

---

Yes  No

Is access to all secured areas where confidential, individual-level HIV/VH/STD/TB information and data are stored limited to persons who are authorized within policies and procedures (this includes access by cleaning or maintenance staff)?

---

#### STANDARD 4.5

---

Yes  No Do policies include procedures for securing documents containing PII when they cannot be returned to a secure work site by the close of business?

---

Yes  No Do policies outline specific reasons, permissions and physical security procedures for using, transporting and protecting documents containing PII in a vehicle or personal residence?

---

Yes  No If no such procedure exists, is approval obtained from the program manager?

---

#### STANDARD 4.6

---

When identifying information is taken from secured areas and included in on-line lists or supporting notes, in either electronic or hard-copy format:

Yes  No

- is it assured that the documents contain only the minimum amount of information necessary for completing a given task?, and
- is the information encrypted?, and
- is it coded to disguise information that could be easily associated with individuals?

---

Yes  No Do staff members in your program ensure that terms easily associated with HIV/VH/STD/TB do not appear anywhere in the context of data transmissions, including sender and recipient addresses and labels?

---

## 5.0 ELECTRONIC DATA SECURITY

#### STANDARD 5.1

---

Yes  No In your program, are HIV/VH/STD/TB analysis data sets stored securely using protective software (i.e., software that controls the storage, removal, and use of the data)?

---

Yes  No Are personal identifiers removed from HIV/VH/STD/TB analysis data sets whenever possible?

---

**STANDARD 5.2**

---

In your program, do transfers of HIV/VH/STD/TB data and information and methods for data collection:

Yes  No

- have the approval of the ORP?, and
  - incorporate the use of access controls?, and
  - encrypt individual-level information and data before electronic transfer?
- 

Yes  No

When possible, are databases and files with individual-level data encrypted when not in use?

---

**STANDARD 5.3**

---

Yes  No

Does your program have a policy that outlines procedures for handling electronic information and data (including, but not limited to, e-mail and fax transmissions) which may contain confidential information that are sent electronically to or from the program?

---

Yes  No

When individual-level HIV/VH/STD/TB information or data are electronically transmitted and the transmission does not incorporate the use of an encryption package meeting the encryption standards of the National Institute of Standards and Technology and approved by the ORP, are the following conditions met?

- The transmission does not contain identifying information.
  - Terms easily associated with HIV/VH/STD/TB do not appear anywhere in the context of the transmission, including the sender and recipient address and label.
-

**STANDARD 5.4**

---

For all laptop computers and other portable devices (e.g., personal digital assistants [PDAs], other handheld devices, and tablet personal computers [tablet PCs]), which receive or store HIV/VH/STD/TB information or data with personal identifiers, are all the following steps taken to ensure the security of the data?

Yes  No

- The devices have encryption software that meets federal standards.
  - Program information with identifiers is encrypted and stored on an external storage device or on the laptop's removable hard drive.
  - External storage devices or hard drives containing the information are separated from the laptop and held securely when not in use.
  - The decryption key is kept some place other than on the device.
- 

Yes  No

Do the methods employed for sanitizing a storage device ensure that the information cannot be retrieved using "undelete" or other data retrieval software?

---

Does the program have policies or procedures to ensure that all removable or external storage devices containing HIV/VH/STD/TB information or data that contain personal identifiers:

Yes  No

- include only the minimum amount of information necessary to accomplish assigned tasks as determined by the program manager, and
- are encrypted or stored under lock and key when not in use, and
- are sanitized immediately after a given task (excludes devices used for backups)?

Where are these policies or procedures stored? \_\_\_\_\_

---

Yes  No

Are hard drives that contain identifying information sanitized or destroyed before the computers are labeled as excess or surplus, reassigned to nonprogram staff members, or sent off site for repair?

---

**STANDARD 5.5**

---

Yes  No

Does your program have policies for handling incoming and outgoing facsimile transmissions to minimize risk of inadvertent disclosure of PII?

---