8: Data Security and Confidentiality

Definitions

Term	Definition
Data confidentiality	The protection of personally identifiable information collected by public health organizations.
Data security	The protection of public health data and information systems to prevent unauthorized release of identifying information and accidental loss of data or damage to the systems.
Overall Responsible Party (ORP)	High-ranking official who accepts overall responsibility for implementing and enforcing data security standards. This official should have the authority to make decisions about program operations that might affect programs accessing or using the data, and should serve as a contact for public health professionals regarding security and confidentiality policies and practices. The ORP is responsible for protecting data as they are collected, stored, analyzed, and released and must certify annually that all security program requirements are being met. The state's security policy must indicate the ORP(s) by name.
Personally identifiable information (PII)	Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Quality Assurance Process for Data Security and Confidentiality

Primary Purpose

This chapter describes the process for maintaining security and confidentiality of TB surveillance data.

- **Security:** To prevent unauthorized release of personally identifiable information **(**PII) and accidental data loss or damage to the systems. The measures to ensure security of data include detecting, documenting, and countering threats to data confidentiality or the integrity of data systems.
- **Confidentiality:** To ensure that PII is not released without the consent of the person involved, except as necessary to protect public health.

QA Process for Data Security and Confidentiality

The CDC Cooperative Agreements (CoAg) with state/local TB programs require that policies and procedures must be in place to protect the confidentiality of all TB surveillance case reports and files. TB programs should also collaborate with HIV/AIDS programs to conduct at least annual TB and AIDS registry matches to ensure completeness of reporting of HIV and TB coinfected patients to both surveillance systems.

Chapter 9: Quality Assurance Cross-cutting Systems and Process provides additional tools and systems (i.e., the National Tuberculosis Indicators Project [NTIP]; Tuberculosis Genotyping System [TB GIMS]; and Cohort Review) that can be used for improving data security and confidentiality.

The quality assurance (QA) process for conducting Data Security and Confidentiality in the CoAg is listed below in Table 8.1

Table 8.1
Data Security and Confidentiality Quality Assurance Process
CoAg Requirements

Note: The requirements are based on the Fiscal Year 2014 CoAg and may need to be updated when the CoAg is updated. The CoAg is reformatted into the following tables with an addition of possible data sources and activities.

CoAg Requirements	Description	Possible Data Sources and Activities
Ensure that TB surveillance data are kept confidentially and that all data files are secure. **Adhere to the Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs.**	**Policies and procedures must be in place to protect the confidentiality of all surveillance case reports and files.**	• Write data security and confidentiality policies and procedures of the TB program. • Review surveillance case reports and files.
	Policies and procedures to protect HIV test results, • Must conform to the confidentiality requirements of the state and local HIV/AIDS programs.	• Review confidentiality requirements of the state and local HIV/AIDS programs. • Develop data security and confidentiality policies and procedures to protect HIV test results. • Observe how staff comply with the policies and procedures.
	Provide training on security and confidentiality of data.	

Example: Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs

Primary Purpose

This section provides a brief overview of the data security and confidentiality guidelines developed by the combined efforts of NCHHSTP's Surveillance Workgroup members, composed of surveillance leaders from NCHHSTP's Division of HIV/AIDS Prevention (DHAP), Division of Viral Hepatitis (DVH), Division of STD Prevention (DSTDP), and Division of Tuberculosis Elimination (DTBE). The work was informed by consultation with state and local public health leaders and public health organizations representing HIV, viral hepatitis, STD, and TB disease disciplines.

This guidance supersedes previously published security and confidentiality guidelines for HIV surveillance and establishes data security and confidentiality standards for viral hepatitis, STD, and TB. Establishment of these standards apply to all surveillance activities in all of the Center's divisions and will facilitate collaboration and service integration among NCHHSTP-funded programs with minimal risk of inappropriate release of confidential, identifiable surveillance data or misuse of those data in pursuit of legitimate public health purposes.

The process for maintaining data security and confidentiality includes seven main steps:

1. Designating an Overall Responsible Party (ORP)
2. Performing a standards-based initial assessment of data security and confidentiality protections
3. Developing and maintaining written data security policies and procedures based on assessment findings
4. Developing and implementing training
5. Developing data-sharing plans or agreements as needed
6. Certification of adherence to standards
7. Performing periodic reviews of policies and procedures.

NCHHSTP-funded programs will also be required to verify their adherence to the standards through submission of certification statements. CDC will work with state, tribal, and local health departments to monitor the implementation of the guidelines and evaluate their impact on securing data, facilitating data use, and increasing program effectiveness.

Additional Information

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. Available at http://www.cdc.gov/nchhstp/programintegration/docs/PCSIDataSecurityGuidelines.pdf.

Exercises 8.1-8.2: Maintaining Data Security and Confidentiality When Coordinating Patient Care and Collecting Surveillance Data

Mario is referred to a small TB clinic at the Laredo County Health Department by Dr. Garcia, his primary care provider. The referral letter requests that he be evaluated to rule out TB disease. Dr. Garcia's referral records indicated that Mario is positive for HIV, hepatitis C, and gonorrhea. From the diagnostic work-up, Dr. Llamas, the physician at the TB clinic, determines that Mario has TB disease.

Helen, the TB clinic nurse, is also the TB surveillance coordinator at the health department. She is entering the TB surveillance data from Mario's medical records into the clinic computer when Dr. Llamas calls her for an emergency. She jumps up to help him in the exam room. She and Dr. Llamas return to the computer and find Mario's neighbor Hector reading Mario's personally identifiable information (PII) on the computer screen.

8.1	**What should Dr. Llamas and Helen do?**
8.2	**How can they prevent this from happening in the future?**

Data Security and Confidentiality Tools

The Data Security and Confidentiality Tools are listed below (Table 8.2). Examples of the tools are located in Chapter 10: Toolkit for Quality Assurance. To view or download the tools, please visit:
http://www.cdc.gov/tb/programs/rvct/default.htm.

Table 8.2
Data Security and Confidentiality Tools

Tool #	Tool Name	Description and How to Use	Format	Source Contact
Data Security and Confidentiality –1	**Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, STD and TB Programs – Standards**	A list of the minimum standards required for data sharing and use of surveillance data for public health action	Word 3 pages	CDC/ NCHHSTP
Data Security and Confidentiality –2	**Data Security and Confidentiality Initial Assessment**	Guidelines on how to initially assess the TB program's data security and confidentiality policies and procedures	Word 3 pages	CDC/ NCHHSTP
Data Security and Confidentiality –3	**Data Security and Confidentiality Periodic Assessment Checklist**	Checklist for conducting ongoing assessment of TB program compliance with the data security and confidentiality guidelines	Word 12 pages	CDC/ NCHHSTP
Data Security and Confidentiality –4	**Data Security and Confidentiality Guidelines Frequently Asked Questions**	Questions and answers to clarify issues regarding the Data Security and Confidentiality Guidelines	Word 5 pages	CDC/ NCHHSTP
Data Security and Confidentiality –5	**Data Security and QA Checklist**	Checklist for data security and QA activities	Word 1 page	California Tuberculosis Control Branch, California Department of Public Health