Annual Security and Confidentiality Training

Insert Name of Your Program

Your name
Your Title
Current date

Annual Security and Confidentiality Training

Acknowledgments:

Provide Acknowledgments If Needed

Objectives

- Introduce current NCHHSTP Data Security and Confidentiality (S&C) guidelines.
- Initiate the process of developing or updating written surveillance systems (hepatitis, HIV, STD, and TB) S&C guidelines.
- Initiate the process of developing written guidelines for data sharing across surveillance systems.

Legal Background

- **Federal Regulations.** At the national level, HIV information is protected by a Federal Assurance of Confidentiality under Section 308(d) of the Public Health Service Act, 42 U.S.C. 242m(d), that prohibits disclosure of identifiable information that could be used to directly and indirectly identify individuals.

Legal Background

- Local Regulations: Insert here

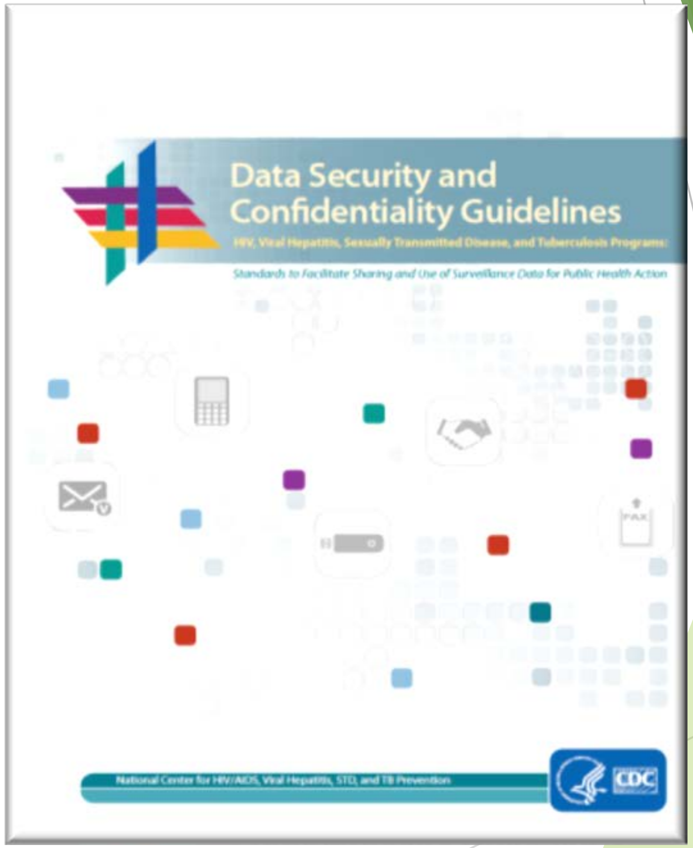
Insert wording of your local law that requires reporting of HIV/hepatitis/TB/STDs and other communicable diseases and covers confidentiality of personal information

Grantees' Responsibilities

- The CDC requires all federally funded Viral Hepatitis/HIV/STD/TB Surveillance programs (Funding Opportunity Announcement PS18-1801) to have a security and confidentiality policy that is in full compliance with the *National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention's (NCHHSTP) Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs (2011)*

2011 NCHHSTP Data Security and Confidentiality Guidelines

- Establishes standards to ensure appropriate collection, storage, sharing, and use of data across surveillance and program areas for the National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention (NCHHSTP).
- Replaces previous guidelines for HIV surveillance programs and establish standards for Viral Hepatitis, STD and TB programs.
- Implementation of common standards across programs will allow for increased use of HIV/ hepatitis/ STD/TB surveillance data for public health action.



Data Security and Confidentiality Guidelines

HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs:

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

National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention

Ten Guiding Principles

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 (PII) necessary to conduct public health activities.
3. Programs should have strong policies to protect the privacy and security of PII.
4. Data collection and use policies should reflect respect for the rights of individuals and community groups and minimize undue burden.

Ten Guiding Principles (Continued)

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 and may establish data-use agreements to facilitate sharing data in a timely manner.

Ten Guiding Principles (Continued)

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.

Definitions

- Confidential Information
- Personally Identifiable Information
- Security
- Overall Responsible Party (ORP)
- Breach of Confidentiality

Confidential Information

- Any private information about an identifiable person who has not given consent to make that information public, or any person whose identity was learned through a case investigation, case report, personal interview, database, or research study.

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.”

Source: National Institute of Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), available at http://csrc.nist.gov/publications/

Personally Identifiable Information (PII) (continued)

- Direct identifiers – e.g., name, social security number or other information that is unique to an individual.

- Indirect identifiers – e.g., uncommon race, ethnicity, extreme age, unusual occupation and other details, especially in combination with each other or other information.

Security

- 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. Security measures include measures to detect, document, and counter threats to data confidentiality or the integrity of data systems.

Security

- Physical Security
  - Personally identifiable program and surveillance data and information must be maintained in a physically secure environment, such as restricted access area with locking file cabinets.

- Electronic Data Security
  - Identifiable electronic data will be held in a technically secure environment, with the number of data locations and individuals permitted access kept to minimum.

Overall Responsible Party (ORP)

- Designated individual who is ultimately responsible for the security and confidentiality of HIV/VH/STD/TB surveillance information. The ORP in the **insert name of your program** is **insert name of your ORP**.

Breach of Confidentiality

A release or disclosure of personally identifiable information to unauthorized persons (e.g. employees or members of the general public) that is not authorized by the Overall Responsible Party (ORP) as defined in Security and Confidentiality Policy.

Security & Confidentiality Training

- CDC mandates annual training for all authorized staff funded under NCHHSTP cooperative agreements.
- All employees, including contractors, are required to sign a confidentiality agreement as new employees and annually thereafter.
- Data security, confidentiality, breaches of confidentiality, and personal responsibility will be covered in the training.
- Secure and confidential collection, storage, use, and transmission of Viral Hepatitis/HIV/STD/TB case information is central to surveillance success.
- No manual or training can cover everything. Ask your supervisor for guidance when a issue is unclear.

Confidentiality Agreement

- CDC mandates that all staff that have access to identifiable information (including IT, mail room, and even custodial staff as necessary) should sign a nondisclosure, confidentiality agreement or oath as new employees and annually thereafter.
- The confidentiality agreement states that the employee agrees not to release PII to any unauthorized persons.
- The agreement should be maintained in the employee's personnel file.
- A confidentiality agreement should be required before assigning passwords or keys that allow access to PII.
- Policies and procedures should address staff out-processing and relinquishment of authorized access.

Physical Security and Data Movement

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

Minimum Secure Area:

- Work space with limited access for only necessary staff
- Locked file cabinets that are large and heavy enough to render them immobile
- A designated location within the work space where confidential conversations may be held

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

- Crosscutting features are needed to ensure confidential information cannot be recovered.
- If a commercial shredding service is used, be sure that documents are shredded on site and in the presence of a staff member.
- In all cases, a contract shredding or disposal company must be bonded, and due diligence should be taken in the selection of the company.

Acceptable Ways to Destroy Paper Documents

- Corporate shredding services – if done on site and witnessed by Health Department staff
- Manual shredding by Health Department staff

4.3: Ensure that data-security policies and procedures address records and data retention

- Question for the group: How long should you keep Viral Hepatitis/HIV/STD/TB-related test information?
- Records retention policies vary by agency- know yours.
- If electronic copies exist, paper copies can be destroyed when no longer needed, in accordance with established policies (if applicable).
- Provisions should be made to destroy copies using methods described in Standard 4.2.

The HIPAA Privacy Rule

- The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

Source: Retrieved April 7, 2017 from https://www.hhs.gov/hipaa/for-professionals/privacy/index.html?language=es

Important!

- Paper copies of any protected health information can constitute a security risk if they are lost or misplaced.

- Avoid a Health Insurance Portability and Accountability Act (HIPAA) violation and destroy paper records per your local records retention policy!

Physical Security

- Rooms containing public health data should not be easily accessible by window.
- If people can potentially see through windows, close blinds when using the computer.
- Monitor screens provide an additional level of security.

All rights reserved to ramimeiri.com 2005

4.5: Ensure that documents containing public health data used by field staff are adequately protected

- Simple physical theft is a major cause of health information breaches.
- Transportation and use of public health data outside of secure areas should, therefore, be minimized and carefully controlled.
- Programs employing field workers should establish specific procedures for:
  - Working with PII outside of secure areas.
  - Obtaining or documenting a manager’s approval to do so.

Insert slide with your specific procedures for working with PII in the field after this slide

4.5: Ensure that documents containing public health data used by field staff are adequately protected (Continued)

- Physically securing documents containing PII that remain in staff custody after usual work hours:
  - Client information with public health data should not be taken to private residences unless specific documented permission is received from the ORP.
  - Policies should include how these data will be protected when not in the office.

Physical Security

- Restricted Access Area

- A secured area with limited access for authorized staff only.

- Includes the work stations and computers of authorized staff.

- Includes locked file cabinets and cross-cut shredders used to destroy paper files.

Physical Security (Continued)

- Hard (Paper) File Storage
- Confidential data must be stored filing cabinets heavy enough to render them immobile with a lock.
- Keys to the locks should be stored in a manner to protect security and prevent unauthorized duplication.
- Duplicate information should NOT be maintained.

Physical Security (Continued)

- Staff Responsibilities
  - Ensure confidentiality of individual workstations.
  - “Clean Desk” Policy – Any loose paperwork containing sensitive information should be cleaned off desktop and locked securely in a drawer when you leave office and at end of every workday.
  - Lock computer screen every time leaving the computer, even for a few minutes.
  - Wear employee Identification badge.
  - Properly destroy documents containing confidential information when no longer needed.

Electronic Data Security

- Computers, Fax Machines, and Printers
  - Always use passwords with a minimum of 7 characters comprised of numbers and letters.
  - Do NOT share passwords with anyone.
  - Do NOT sign on and allow someone else to access data.
  - Restrict printer and fax access space. If fax machines are used, they should be maintained in a secure locked space. Guidelines for us of FAX provided in Appendix F. of NCHHSTP Guidelines.
  - Only use printers that do NOT store information on an internal hard drive.

Electronic Data Security (Continued)

- Electronic Databases
  - Electronic databases should be maintained on secure servers with backups preformed regularly on secure servers.
  - Only required staff should have access to databases with the minimum level of access granted to fulfill job responsibilities (i.e., read only access).
  - Do NOT share passwords with anyone.
  - Do NOT sign on and allow someone else to access data.
  - Once access is no longer required, user accounts should be deactivated.

Electronic Data Security (Continued)

- Electronic Databases
  - Data should be encrypted if removed from the secure server and always encrypted before transfer.
  - Encryption is still recommended for a data system if it is located on a secure separate server.
  - Back-ups should be encrypted, if possible, before being copied to a secure location.

Electronic Data Security (Continued)

- Destruction of Data
  - Computer disks and hard drives are wiped prior to destruction.
  - Hard drives of computers, scanners, and copy machines should be physically removed and destroyed.

Digital Photocopiers and Data Security

http://www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets/

- The link above provides an illustration of why securing PII is important, even the use of photocopy machines can put people at risk of having their personal information exposed.
- Bottom Line: Organizations should ensure that all PII is protected, particularly in places where they are least suspected of being released someday - photocopy machines.

Data Security

- All discussions pertaining to confidential information are conducted in secure private areas. Medical record reviews are conducted as discreetly as possible.

- Confidential information is never left in public or general access areas.

- Analysis datasets are held in secure restricted access locations.

- Surveillance information must have personal identifiers removed and must be encrypted before electronically transferring to CDC and other health partners agreeing to keep data secure.

Data Security (Continued)

- **Mail**
  - **Outgoing:** Managed by the health department and U.S. federal mail. All confidential information is placed in double envelopes, with “Confidential” marked on the inner envelope. No envelope should have any direct or indirect reference to any disease.
  - **Incoming:** Only designated staff opens program mail and distributes to appropriate supervisor. Reports are filed on a locked cabinet.

Data Security (Continued)

- **Electronic Communication**
  - Faxing identifiable information should be avoided. Programs should minimize the inclusion of PII, and if faxing is necessary, all steps should be taken to minimize the risks when using a fax (refer to 2011 Guidelines pp. 33 and 61, Appendix F).
    - https://www.cdc.gov/nchhstp/programintegration/data-security.htm
  - Email is NOT used to transmit confidential information.

Data Security (Continued)

- **Incoming Telephone Calls**
  - Generic identifiers (e.g., “Department of Health, this is Name”), without direct reference to the particular disease(s) are used to answer all incoming calls.
- **Outgoing Telephone Calls**
  - Surveillance staff should discuss confidential information so as not to be overheard by others, release information to only those individuals with a need-to-know, and always use utmost discretion.

Data Security (Continued)

- **Cellular Phone Service**
  - Cellular phone transmission is NOT secure. Never use patient-identifying information during a cellular phone call. Callers should refer to specific individuals by stateno or some other reference that is familiar to the recipient of the information. If patient-identifying information must be shared, the caller should return the call from a land line telephone.
  - Cell Phone and PDA Security, National Institute of Standards and Technology Special Publication 800-124 [Natl. Inst. Stand. Technol. Spec. Publ. 800-124, 51 pages (Oct. 2008), http://csrc.nist.gov/publications/] when developing policies.

Data Release Policy

- A Data Release Policy for the program describes the roles and responsibilities of program personnel, including any confidentiality agreements and training they must receive.
- The policy describes:
    - Access procedures and authorization rules
    - Descriptions of the data and to whom, and in what format, they can be released
    - Procedures for data release
    - Specific requirements for sharing identifiable data
    - Mechanisms for data release, including rules for minimizing disclosure such as cell-size restrictions (needed when the number of cases are very small)
    - Disposition of data after they have been used for a stated purpose
- Data release plans should include mechanisms for evaluating the usefulness of released data and whether the release of data is causing undue burden on individuals or communities.

Breach of Confidentiality

- A breach of confidentiality is an unauthorized release or disclosure of personally identifiable information (PII) that is not authorized by the Overall Responsible Party (ORP).

  Example: Releasing PII outside of your job responsibilities.

- Report all breaches or suspected breaches of confidentiality immediately to your supervisor or ORP.
- The ORP is to be notified as soon as possible after the event occurs; within the same day if possible.
- Report breaches to your CDC Epidemiologist and Project Officer too.

Breach of Confidentiality (Continued)

- Unauthorized release of PII from a federally supported data system must be reported to CDC within one hour of discovery to the NCHHSTP Information System Security Officer (ISSO).
- Notify your CDC program project officer or epidemiologist who can assist you with required reporting.
- See Standard 1.5 of the NCHHSTP Data Security and Confidentiality Guidelines for more information regarding policies and procedures related to breaches in confidentiality.

Breach of Confidentiality (Continued)

- **Staff Responsibilities**
  - Example: All staff authorized to handle Surveillance information will immediately report all breaches or suspected breaches of confidentiality to the appropriate Surveillance Coordinator who will then immediately notify the ORP.
  - This applies to all public health information including HIV, TB, STD, and hepatitis.

Breach of Confidentiality (Continued)

- **Penalty for unauthorized release of information**
  - Breach of security and confidentiality pertaining to confidential Surveillance information may result in suspension, demotion, or termination based on the severity of the offense. The severity of the offense and appropriate disciplinary action for all **insert program name** staff with access to surveillance information will be determined by the ORP, HR, and the Legal Affairs Office.
  - **Give your program's disciplinary action here**

Remember

- Security & Confidentiality is EVERYONE’S responsibility. Exercise good judgment in the daily management of all public health information.
- As public health workers, we have an obligation to conduct our jobs in a manner that protects the confidentiality of clients infected with HIV/STD/TB/hepatitis or other diseases, and to maintain the public trust.
- Destroy data if it is no longer needed.

Who to Contact?

Insert name of ORP
ORP email
Telephone: ORP number

Your Supervisor