HIV/AIDS Surveillance Security & Confidentiality Training

HIV/AIDS Surveillance Program
Division of STD and HIV
Office of Epidemiology and Prevention Services
Bureau for Public Health
West Virginia Department of Health & Human Resources

Prepared by: Amy Atkins, MPA

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

Objective

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Provide an overview of the West Virginia DHHR HIV/AIDS Surveillance Program security standards
  - Developed by the CDC in collaboration with CSTE
  - *Technical Guidance for HIV/AIDS Surveillance Programs Volume III: Security and Confidentiality*
  - Standards presented apply to:
    - All staff and contractors funded through CDC to perform HIV/AIDS surveillance
    - All sites where HIV/AIDS reporting systems is mandated
  - Available on the CDC website:

    CDC Data Security and Confidentiality Guidelines

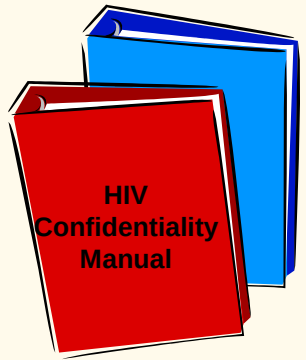
Legal Background

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Federal laws:
  - Federal assurance of confidentiality under sections 306 and 308(d) of the Public Health Service Act, which prohibits disclosure of any information that could be used to identify patients
- State laws:
  - West Virginia Code §16-3C-8, §16-3-C-1, and Legislative Rules 64 CSR 64, 1996, and 64 CSR 7, 2006
  - Patient name, demographic data and disease information are required on the (HIV or AIDS) case report but further disclosure of this information is prohibited by law without written consent by the patient

Policies

- Confidentiality & Security Policies and Requirements are in writing
  - WV HIV/AIDS Program Security & Confidentiality Policy Manual
    - Hard copy in HIV/AIDS Surveillance Office
    - Electronic copy available on the S drive
- Each member of the surveillance staff must be knowledgeable about the HIV/AIDS Program security and confidentiality policies and procedures



5 Guiding Principles

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- 5 guiding principles are the backbone upon which all security considerations are derived
  1. HIV/AIDS data will be maintained in a physically secure environment
  2. Electronic data will be held in a technically secure environment with minimum access
  3. Staff with authorized access will be responsible for protecting confidential data
  4. Security breaches will be investigated thoroughly with sanctions when appropriate
  5. Security practices and written policies will be continuously reviewed and changed to improve protections

Program Requirements

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Mandated by CDC as a condition of funding
- Minimum standard that all HIV/AIDS Program surveillance staff must achieve
  - Falling below this standard could result in corrective action
  - Disciplinary action may range from an employee reprimand to criminal charges
- Certified annually by the Overall Responsible Party (ORP) Panel
  - WV ORP Panel Contact: William Hoffman
    William.C.Hoffman@wv.gov (304) 356-4054

Confidentiality Agreement

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Access to the HIV/AIDS Program surveillance office, hard copy files containing patient information, and other HIV/AIDS data is limited to authorized personnel on the basis of a justifiable public health need, as determined by the ORP
- Individuals granted access must sign the HIV/AIDS Program Confidentiality Agreement
  - New HIV/AIDS Program Surveillance Staff must sign the agreement prior to data access
  - All authorized staff must annually sign the agreement

Training

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- HIV/AIDS Program surveillance staff with access to confidential surveillance data must attend security training
  - Upon hire and annually thereafter
  - Documented in the employee's personnel file
- Non-HIV/AIDS Program staff who require access to confidential surveillance data must undergo the same training and sign the same confidentiality agreements

Confidential Information

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- All HIV/AIDS records are strictly confidential
- Only HIV/AIDS surveillance personnel have access to confidential records and databases
- Access to confidential information by individuals outside the HIV/AIDS surveillance team must be limited to those with a justifiable public health need
  - No identifying information is released to offices in the state with the exception of the West Virginia DHHR STD Program for confidential Partner Services
  - Confidential information may be released to known out-of-state HIV/AIDS Surveillance staff for reporting purposes

Data Release

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- No HIV/AIDS public dataset exists; therefore, all data is requested
- A data request form must be completed and forwarded to the DSH Assistant Director and the Programmer Analyst
- All HIV/AIDS data is released with no personal identifiers
- Aggregate statistical data are only released in published reports when the number of cases meeting the selection criteria, or cell size (or geographic area), is greater than or equal to 5 or where the population is less than 100 persons.
  - Release of cells (or geographic areas) containing <5 cases may occur in reports approved by the ORP for internal use only and not for public release!

Responsibilities of Staff

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Must be knowledgeable about other applicable West Virginia DHHR information security policies and procedures
- Must protect their workstation, laptop, and/or other devices associated with confidential HIV/AIDS information
  - Protect keys, passwords, etc.
  - Protect computer monitors from being observed by unauthorized personnel
  - Not infect computer with viruses

- Must challenge any unauthorized users of the data and report any breaches of confidentiality or security

Physical Security

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- All physical locations containing electronic or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access
  - Not easily accessible by window
- Paper copies of confidential information must be stored inside locked file cabinets inside a locked room
  - Shred confidential documents when no longer needed

Physical Security (cont.)

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Workspace for individuals with access to surveillance information must be within a secure area with computer screens protected from view
- When the HIV/AIDS surveillance office is unattended, staff ensure case reports, laboratory reports, and any other materials which contain confidential information on HIV/AIDS cases are placed in a locked file cabinet, computer screens cleared, and the office locked
- The last person leaving the secured area is responsible for locking all file cabinets and the door before leaving

Data Security

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Surveillance data must have personal identifiers removed if taken out of the secured area or accessed from an unsecured area
- Documents taken from secured areas must contain only the minimum amount of information necessary for completing a given task and, if possible, must be coded to disguise any information that could easily be associated with HIV/AIDS
- In the field, staff must keep confidential data with them at all times
  - If not possible, material may be kept in a locked room/file cabinet at the site or under the direct supervision of site staff
  - Confidential material provided by hospitals/clinics is never removed from these sites

Data Security (cont.)

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Confidential HIV/AIDS information is returned to the office at the end of the day
- Prior approval must be obtained from the HIV/AIDS Surveillance Coordinator when planned travel prevents the return of information to the secured area on the same day
- HIV/AIDS surveillance information with personal identifiers must not be taken to private residences unless written permission is received from the HIV/AIDS Surveillance Coordinator
  - Data may be taken to private residences without approval if an unforeseen dangerous situation arises (i.e. heavy snowstorm)
  - Precautions must be taken at the workers' home to protect HIV/AIDS information (i.e., case report forms and computers hard drive stored in locked briefcase)

Data Security (cont.)

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- The person to whom the mail is addressed may only open mail
  - Mail not addressed to a specific person is opened by the HIV/AIDS Secretary
- Outgoing mail should not contain the words ‘HIV’ and/or ‘AIDS’ in the mailing or return address and is stamped, “CONFIDENTIAL”
- Line lists should not be mailed
- HIV/AIDS surveillance staff must not send letters, leave business cards, or record voice messages at the person’s residence that includes any terminology that could be associated with HIV/AIDS
- The use of fax for electronic transfer of confidential data is **NEVER** allowed

Data Security (cont.)

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Telephone communication of confidential information is made only to familiar, authorized individuals (e.g. providers, out-of-state HIV/AIDS surveillance staff) on a need-to-know basis
- Telephones should be answered by the HIV/AIDS Program surveillance staff with generic identifiers (i.e. “Office of Epidemiology and Prevention Services”) without any direct reference to HIV/AIDS
- Access to Internet or Internet based email is prohibited when accessing HIV/AIDS surveillance information, because accidental transmission of data can occur
- Wireless Fidelity (Wi-Fi) is not completely secure and should never be used

Password Protection

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- HIV/AIDS Surveillance staff are required to have a unique login name and password in order to access their computers
- Passwords protect the data stored on your computer system
  - Don't use a password easily obtained about you (e.g., DOB)
  - Don't share your password or write it down
  - Use a combination of letters/numbers/characters
  - Don’t reuse old passwords
- If your password is stolen or becomes known to another person, notify your supervisor immediately

WEST VIRGINIA
Department of
Health & Human Resources
BUREAU FOR PUBLIC HEALTH

TREAT YOUR PASSWORD LIKE A TOOTHBRUSH

DON'T SHARE THEM & GET A NEW ONE EVERY MONTH!

Sending Electronic Data

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Data transmitted electronically
  - Must be encrypted
  - Ancillary databases must be encrypted when not in use
  - Meet the Advanced Encryption Standard (AES)
  - Not contain terms easily associated with HIV/AIDS

Access Control

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Only HIV/AIDS Program surveillance staff are allowed to enter the secured areas
  - Unauthorized individuals are granted access when authorized surveillance personnel are available for escort
  - Staff are to question any strangers that enter the secured area and report immediately to the DSH Director and Assistant Director any suspicious behavior
- Access to surveillance information with identifiers by those who maintain other disease data stores must be limited
  - Linkages with other disease registries (i.e. Cancer, TB, STD) are conducted at the HIV/AIDS Program office by the Programmer Analyst

Access Control (cont.)

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Confidential information is never released to insurers, employers, landlords, other health department staff or any other person for any reason
- Confidential patient information may be released to known out-of-state HIV/AIDS surveillance staff for reporting purposes
- Access to HIV/AIDS surveillance information for nonpublic health purposes, such as litigation or court order, must be granted only to the extent required by law
- Court orders, subpoenas, or other requests for HIV/AIDS information are referred to the HIV/AIDS Surveillance Coordinator, the DSH Director, the DSH Assistant Director, and the ORP

Security Breaches

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- All staff are responsible for reporting suspected security breaches to the ORP, the DSH Director, the DSH Assistant Director, and the Surveillance Coordinator
- A breach that results in the release of private information (breach of confidentiality) should also be reported to the Team Leader of the Reporting, Analysis, and Evaluation Team (DHAP, NCHSTP, CDC)
- A suspected breach of confidentiality must be immediately investigated to implement remedies
- In consultation with legal counsel, surveillance staff should determine whether a breach warrants reporting to law enforcement agencies

Examples of Security Breaches

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Leaving case information out on your desk after you go home for the day
- Discussing confidential information over the telephone while others who should not have access to this information are around
- Not logging off your computer when you leave your workstation
- Checking records of people you know

Consequences of Security Breaches

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- West Virginia DHHR staff who violate confidentiality and security policies are subject to disciplinary actions
  - Corrective counseling/Written reprimands
  - Suspension of data privileges
  - Suspension from duty
  - Termination
  - Civil penalties
  - Criminal prosecution

Electronic Storage Devices

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Laptops, Portable Devices (e.g. PDAs), and other external storage devices that receive or store surveillance data must incorporate the use of encryption software
  - Surveillance data must be encrypted when not in use
  - The decryption key must not be on the laptop/storage device
- Only contain the minimum amount of information necessary to accomplish the job duties

Electronic Storage Devices

WEST VIRGINIA Department of Health & Human Resources
BUREAU FOR PUBLIC HEALTH

- Laptop computers may be used in the field
  - Laptops are only used in private rooms
  - When leaving the laptop unattended, the room is locked
  - Access to laptop programs is password protected
- Hard disks, diskettes, and jump drives that contain identifying information must be cleaned before they are re-used for other purposes and destroyed before disposal

Get Certificate