Security and Confidentiality Training & Guidelines

HIV/STD/VH/TB Epidemiology Section

Communicable Diseases Division

December 7, 2010

Modified 3/2011 for MDSS Users

Introduction

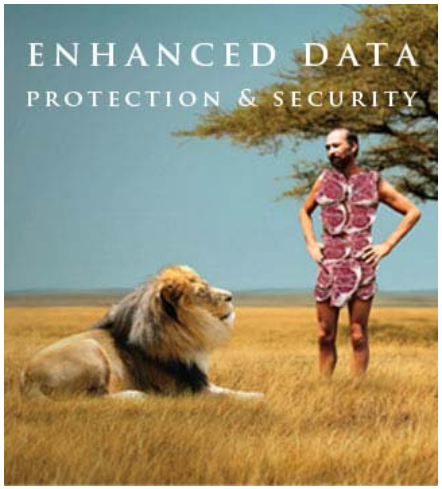
All MDDS users who have HIV Program access should have policies and procedures in place to protect the security and confidentiality of HIV data. In addition users should complete a security and confidentiality training on an annual basis. This training in addition to the MDSS HIV/AIDS Confidentiality Policy are the recommended guidelines for the protection of HIV data within MDSS.

People and Data Protection!

- Alerting end users to Program Policies and educating staff about the importance of keeping information safe is perhaps the most crucial step in preventing a breach of confidentiality. User education must be accompanied by sensible, well-thought-out policies, and those policies must be applied in a way that suits the business at hand.

- People, Policies and Products must work together to avoid data leakage internally as well as externally.

Risks



- Identifiable information is viewed, transmitted or moved in various methods. (electronically, hard copies, fax, etc.)
- Physical access to secure area
- Communications (verbal, electronic, written, email, etc.)

Why are safeguards needed?

Data are sensitive as it involves information on:

- Sexual attitudes, preferences, or practices
- Use of alcohol, drugs, other addictive products
- Illegal conduct
- Individual's psychological or mental health
- Information normally recorded in a medical record, the disclosure of which could lead to social stigmatization

State of Michigan Requirements

- Confidentiality of HIV/AIDS Information (MCL 333.5131)- HIV-related information is confidential and cannot be released unless the patient authorizes disclosure, or a statutory exception applies. This confidentiality statute applies to all reports, records, and data pertaining to testing, care, treatment, reporting and research, and information pertaining to partner services under section 5114a, that are associated with the serious communicable diseases or infections of HIV and AIDS.

State of Michigan Requirements

- No lists of HIV infected individuals should be kept for any reason
  - MCL 333.5114, Section 5114. (4) A Local Health Department shall not maintain a roster of names obtained under this section, but shall maintain individual case files that are encoded to protect the identities of the individual test subjects.

HIPAA

Reporting of Communicable Diseases (including HIV/STD) to the local or state health department are exempt because they are mandated within the Michigan Public Health Code and are used for surveillance and prevention of communicable diseases.

- Examples of Protected health information (PHI)
  - Name
  - Address
  - Telephone numbers
  - Birthdate
  - Medicaid ID number and other medical record numbers
  - Social Security number
  - Name of employer

Physical Security

Physical Security

- Workspace for individuals with access to HIV data and all physical locations containing electronic or paper copies of HIV data should be inside a secured area with limited access

- All staff that are authorized to access HIV data should be responsible for challenging those who are not authorized to access surveillance data

Individual Responsibility

Individual Responsibility

- All authorized staff individually responsible for protecting workstation, laptop, or other devices
- Must protect keys, passwords, and codes
  - Use of alpha-numeric characters in password
  - Never write or store passwords
  - Computer saved passwords disabled
- Confidential paper on desk
  - Should not be face up when you leave your desk

Individual Responsibility

- Conversations about cases personal information
  - Use of names should be kept to a minimum and used only when necessary
- Always know/verify who you are talking to
- Be reluctant to provide information until you are sure you are talking about an actual case with an authorized and appropriate person
- Never email or text patient name or other identifying information

Security Breaches

Security Breaches

- Security Breach
  - Supervisor notified
  - Immediately investigated
- …resulting in release of personal information
  - Attention to legal ramifications
- All staff authorized to access HIV data must be responsible for reporting suspected security breaches
- Training of non-surveillance staff must also include this directive

Handling of Confidential Data

PAPER

Confidential Data: Paper

- State of Michigan Retention Policy
  - CRFs 30 years
  - Notes and pieces of paper Immediately
- Disposal
  - Paper should be shredded (with crosscutting feature) before disposal
  - Shredder bins: pulverized, not ‘shredded’
- Mailing
  - Double envelope, stamped ‘Confidential’ and ‘To be opened by Addressee Only’

Shredding is Good!

Shredders should be of commercial quality with a crosscutting feature.

Confidential Data: Paper

- Paper with SSN must be shredded before recycling
  - Not just names, but consider paper with ANY potential identifying information

Handling of Confidential Data

ELECTRONIC DATA:

USE, STORAGE, TRANSFER

Confidential Data: Electronic Use/Storage

- Databases and files created by staff
  - Saved to a secure restricted location on the server
  - Deleted after final use
  - Only files/databases without names/identifying information should be saved on the desktop
- Each workstation should be configured with a password-protected screen saver, which will lock the computer after 5-10 minutes of non-use
- The use of a privacy filter on the computer monitor to keep private information safe is recommended

Confidential Data: Electronic Transfer

- Electronic transmission of case specific information must either be:
  - Encrypted using software that meets 128-Bit DES encryption standards, -OR-
  - The transmission should not contain identifying information or use terms easily associated with HIV or AIDS, -AND-
  - HIV or AIDS should not appear in the context of communication, or in sender or recipient address or label

Confidential Data: Electronic Transfer

- Encrypted
  - Data Encryption Standard = 128 bit
  - PGP
- DCH Transfer
  - Files not encrypted, but process is
  - Does contain names and ‘HIV’ terms

Handling of Confidential Data

ELECTRONIC DATA:

USE OF EXTERNAL DEVICES

Use of External Devices

- If receiving or storing HIV data with personal identifiers
  - Should be encrypted
- Hard drive containing the data should be removed (if able) when not in use
- Except for devices used for backups, devices should be sanitized immediately following a task

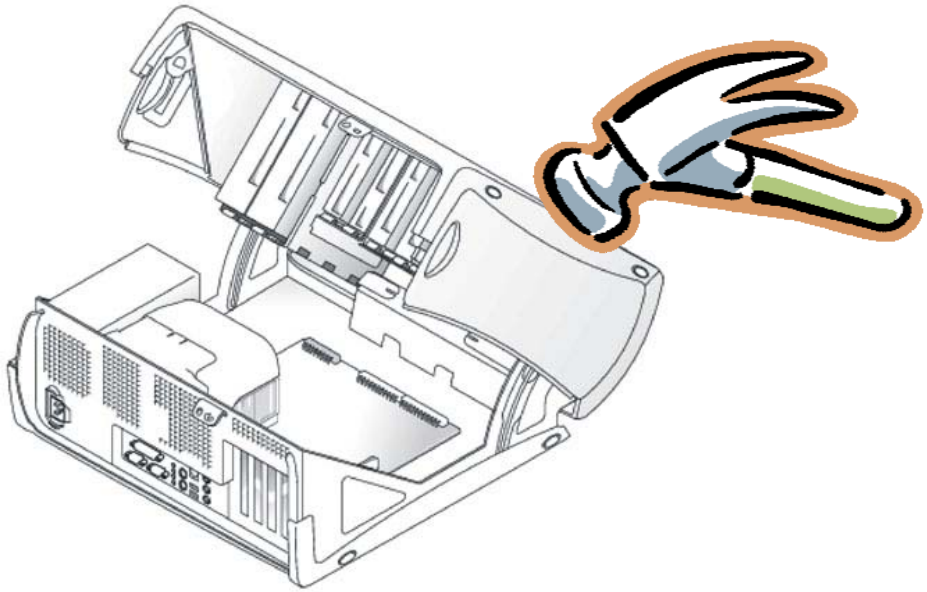
Use of External Devices

(Business or Personal)

- Laptop, tablets, Blackberrys, cellphones, PDAs, IPods, USB/Flash/Jump drives
- Flash/Jump drives
  - Don’t mix home and work files
  - Can be a data security nightmare so NEVER store confidential data here

Use of External Devices

- Hard disks that contained identifying information should be sanitized or destroyed before computers are labeled as excess or surplus, reassigned to a non-HIV Program user, or before they are sent off site for repair



Use of External Devices

(Business or Personal)

- Should not connect foreign devices to network/computer without
  - A “business need”
  - Written approval
- MUST be encrypted if
  - Name, SSN, and any other PHI defined under HIPPA
- Includes State and Privately owned
  - Laptop, tablets, Blackberry’s, cellphone’s, PDA’s, etc.

Penalty for Violation

- 333.5131(8)
- A person who violates this section is guilty of a misdemeanor, punishable by imprisonment for not more than 1 year or a fine of not more than $5,000.00, or both, and is liable in a civil action for actual damages or $1,000.00, whichever is greater, and costs and reasonable attorney fees. This subsection also applies to the employer of a person who violates this section, unless the employer had in effect at the time of the violation reasonable precautions designed to prevent the violation."
- …can result in immediate dismissal

- Thank you for taking the Confidentiality and Security Training.

- It is recommended that MDSS users with access to HIV data review this training once a year.