

Michigan Department of Community Health
Public Health Administration/Bureau of Epidemiology
Communicable Disease Division

HIV/AIDS Surveillance Program Confidentiality and Data Security Policy

Section I: Legal Authority and Requirements

Reporting Law

In Michigan, HIV infection is required to be reported under Michigan Compiled Laws (MCL) 333.5114. AIDS is required to be reported under the Communicable Disease Rules that are promulgated by the Michigan Department of Community Health under MCL 333.5111.

Confidentiality

Both HIV infection and AIDS are designated as “serious communicable diseases or infections” under MCL 333.5101. MCL 333.5131(1) states that, “all reports, records and data pertaining to the treatment, reporting and research associated with [these] serious communicable diseases are confidential and shall be released only pursuant to this section. The exemptions are then listed and they are summarized in the booklet “Michigan HIV Laws, How They Affect Physicians and Other Health Care Workers”.

Penalty for Violation

MCL Section 333.5131(8) states that “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.”

Violation of this written confidentiality and data security policy can result in immediate dismissal. In addition, supervisors may deny access to the named data bases at their discretion until necessary investigation occurs; for example, any employee who has data base access who exhibits questionable use or indiscretion will be denied access.

Section II: Implementation of Policy

This policy will be reviewed annually in October by the security and confidentiality guidelines team and more often as necessary to insure that evolving technologies are reviewed. The IT manager, who is part of the review team, will be charged with the responsibility of reviewing evolving technologies and how they might impact the policy. The Security and Confidentiality Checklist Attachment-H (attached) from CDC’s surveillance guidelines will be used to complete this review. Each review/revision date will be added to the footer of the policy at the time of the review.

Overall Responsible Party (ORP)

The MDCH Deputy Director for Public Health Administration, Jean Chabut, MPH, is designated as the ORP. The ORP accepts overall responsibility for the implementation and enforcement the security standards and may be liable for breaches of confidentiality and has the authority to make decisions about surveillance operations that may affect programs outside the HIV/AIDS surveillance unit.

In compliance with CDC's cooperative agreement, the ORP will certify annually that all program requirements are met. By signing the form annually, the ORP certifies that MDCH complies with the "Security Standards for the Protection of the HIV/AIDS Surveillance Information & Data" by:

- a) Acknowledging that all "**Program Requirements**" included in the CDC "Security Standards for the Protection of HIV/AIDS Surveillance Information & Data" have been implemented.
- b) Applying the "**Program Requirements**" to all local/state/territorial staff and contractors funded through CDC to perform HIV/AIDS surveillance activities.
- c) Applying the "**Program Requirements**" at all sites where the HIV/AIDS Reporting System (eHARS) is maintained.

Section III: Requirements

HIV/AIDS surveillance information (hardcopy) and data (electronic) will be maintained in a physically secure environment.

Electronic HIV/AIDS surveillance data will be held in a technically secure environment, with the number of data repositories and individuals permitted access kept to a minimum. Operational security procedures will be implemented and documented to minimize the number of staff that have access to personal identifiers and to minimize the number of locations where personal identifiers are stored.

Individual surveillance staff members and persons authorized to access case-specific information will be responsible for protecting confidential HIV/AIDS surveillance information and data.

Security breaches of HIV/AIDS surveillance information or data will be investigated thoroughly by the Section Manger, IT Manager/Security Officer and the Epidemiology Manager to assess causes, implement remedies, and impose sanctions as appropriate. All staff authorized to access surveillance data will be responsible for immediately reporting suspected security breaches to their supervisor and/or the Section Manager and Epidemiology Manager. Training of nonsurveillance staff must also include this directive.

A breach that results in the release of private information about one or more individuals (breach of confidentiality) should be reported immediately to the Team Leader of the Reporting,

Analysis, and Evaluation Team, HIV Incidence and Case Surveillance Branch, DHAP, NCHSTP, CDC. CDC may be able to assist the surveillance unit dealing with the breach. In consultation with appropriate legal counsel, surveillance staff should determine whether a breach warrants reporting to law enforcement agencies.

Release of confidential HIV/AIDS surveillance information or data is defined in the data release policy including the provision to restrict the release and public access to raw data or data tables with small denominators that could be indirectly identifying.

This policy will at all times be readily accessible by any surveillance staff having access to confidential surveillance information or data at both the Lansing and Detroit offices.

HIV/AIDS Surveillance staff roles in the Lansing and Detroit offices are the only staff authorized to access confidential HIV/AIDS surveillance information and data. Every individual with access to confidential HIV/AIDS surveillance information and data must attend security training annually. A training program is being developed so that IT staff and contractors who require access to data must undergo the same training as surveillance staff and sign the same agreements. This requirement applies to any staff with access to servers, workstations, backup devices, etc.

All authorized staff must sign a confidentiality statement annually. Initial access for new employees will only be granted after orientation occurs and the policy is reviewed with the employee and the Oath of Confidentiality Form is signed. Access will be granted by the IT manager after the employee's supervisor grants permission and the new employee or newly authorized staff shows the signed confidentiality statement.

The Oath of Confidentiality will include a statement that indicates that the employee understands and agrees that confidential HIV/AIDS surveillance information and data will not be released to any individual not granted access. The signed oath will be held in the employee's personnel file and a copy given to the employee. Each member of the surveillance staff and all persons described in this document who are authorized to access case-specific information must be knowledgeable about other applicable MDCH information security policies and procedures (see attachments).

The amount and sensitivity of confidential HIV/AIDS surveillance information and/or data contained in any one piece of mail will be kept to a minimum. Confidential information is sent in double, tamper resistant envelopes that are stamped "Confidential" and "To be opened by addressee only"; no more than 10 case report forms per envelope.

For example, one envelope should not contain more than 10 case report forms if there are names or addresses written on them. Line lists of names have no restrictions on them as long as there is no way to identify them as HIV-infected. If information about HIV infection is also included then line lists should also contain no more than 10 names per envelope. These guidelines apply to paper only and not to clinical laboratory specimens which have separate guidelines that are developed specifically for the laboratory setting. Confidential HIV/AIDS surveillance information and/or data will be mailed in an envelope addressed to a specific 'named' person and clearly marked as confidential.

All staff who are authorized to access confidential HIV/AIDS surveillance information and data are responsible for challenging those who are not authorized to access surveillance data.

All staff who are authorized to access confidential HIV/AIDS surveillance information and data are individually responsible for protecting their own workstations, other devices, WAN access associated with confidential surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential HIV/AIDS surveillance information or data. Staff must follow guidelines to prevent infecting program computer equipment with computer viruses and not to damage hardware through exposure to extreme heat or cold.

All physical locations containing electronic or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access. Workspace for individuals with access to surveillance information must also be within a secure locked area. Rooms containing confidential HIV/AIDS surveillance information and data must not be easily accessible by window.

Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room. Each member of the surveillance staff must shred documents containing confidential HIV/AIDS surveillance information and data before disposing of them. Shredders must be of commercial quality with a crosscutting feature.

Surveillance information must have personal identifiers removed (an analysis dataset) if taken out of the secured area or accessed from an unsecured area.

An analysis dataset must be held securely by using protective software (i.e., software that controls the storage, removal, and use of the data).

Data transfers and methods for data collection must be approved by the ORP and incorporate the use of access controls. Confidential surveillance data or information must be encrypted before electronic transfer. Encryption of ancillary databases or other electronic files used by surveillance when not in use is currently under review.

When case-specific information that identifies an individual to anyone who would see it is electronically transmitted, any transmission that does not incorporate the use of an encryption package meeting the Advanced Encryption Standard (AES) encryption standards and approved by the ORP must not contain identifying information or use terms easily associated with HIV/AIDS. The terms HIV or AIDS, or specific behavioral information must not appear anywhere in the context of the communication, including the sender and/or recipient address.

When identifying information is taken from secured areas and included on line lists or supporting notes, in either electronic or hard copy format, these documents must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any information that could easily be associated with HIV or AIDS.

Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the surveillance coordinator. Prior approval must be obtained from the surveillance coordinator when planned business travel precludes the

return of surveillance information with personal identifiers to the secured area by the close of business on the same day.

Access to any surveillance information containing names for research purposes (that is, for other than routine surveillance purposes) must be contingent on a demonstrated need for the names, an Institutional Review Board (IRB) approval, and the signing of a confidentiality statement regarding rules of access and final disposition of the information. Access to surveillance data or information without names for research purposes beyond routine surveillance may still require IRB approval depending on the numbers and types of variables requested in accordance with local data release policies.

Access to any secured areas that contains either confidential HIV/AIDS surveillance information or data or can be used to access surveillance data by unauthorized individuals can only be granted during times when authorized surveillance or IT personnel are available for escort or under conditions where the data are protected by security measures specified in a written policy and approved by the ORP.

Access to confidential surveillance information and data by personnel outside the surveillance unit must be limited to those authorized based on an expressed and justifiable public health need, must not compromise or impede surveillance activities, must not affect the public perception of confidentiality of the surveillance system, and must be approved by the ORP.

Access to surveillance information with identifiers by those who maintain other disease data stores must be limited to those for whom the ORP has weighed the benefits and risks of allowing access and can certify that the level of security established is equivalent to the standards described in this document.

Access to surveillance information or data for nonpublic health purposes, such as litigation, discovery, or court order, must be granted only to the extent required by law.

Laptops and other portable devices (e.g., personal digital assistants [PDAs], other handheld devices, and tablet personal computers [PCs]) that receive or store surveillance information with personal identifiers must incorporate the use of encryption software. Surveillance information with identifiers must be encrypted whenever stored on an external storage device or on the laptop's removable hard drive. The external storage device or hard drive containing the data must be separated from the laptop and held securely when not in use. The decryption key must not be on the laptop. Other portable devices without removable or external storage components must employ the use of encryption software that meets federal standards.

All removable or external storage devices containing surveillance information that contains personal identifiers must:

- (1) include only the minimum amount of information necessary to accomplish assigned tasks as determined by the surveillance coordinator,
- (2) be encrypted or stored under lock and key when not in use, and

(3) with the exception of devices used for backups, devices should be sanitized immediately following a given task. Before any device containing sensitive data is taken out of the secured area, the data must be encrypted. Methods for sanitizing a storage device must ensure that the data cannot be retrievable using Undelete or other data retrieval software. Hard disks that contained identifying information must be sanitized or destroyed before computers are labeled as excess or surplus, reassigned to nonsurveillance staff, or before they are sent off-site for repair.