

MICHIGAN DEPARTMENT OF COMMUNITY HEALTH
Division of Health, Wellness & Disease Control

HIV/AIDS Confidentiality and Data Security Guidance
August 2009

The purpose of this document is to provide guidance to local health departments (LHDs) and community based organizations (CBOs) on developing, implementing, and maintaining policies and procedures to protect HIV/AIDS client confidentiality and medical records. Although many agencies have already developed policies, this document may be used to augment and update protocols. This document is not intended to replace the Health Insurance Portability and Accountability Act (HIPAA), but instead provides more detailed and specific information regarding HIV/AIDS clients and how to protect their confidentiality and medical records consistent with the State of Michigan Public Health Code.

Note that several examples of the HIV/AIDS Surveillance Program's (HASP) security system at the Michigan Department of Community Health (MDCH) have been included in the development of this guidance. Copies of the HASP policy, which has substantial detail for protecting electronic records, may be obtained by telephoning (517) 335-8165.

I. Legal Authority for Confidentiality Policies

Both HIV infection and AIDS are designated as "serious communicable diseases or infections" under Michigan Compiled Laws (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." A few exceptions are listed in the booklet "Michigan HIV Laws: How They Affect Physicians and Other Health Care Providers" (January 2006). The booklet is available at the following site: < www.michigan.gov-documents-mihivlaws_49845_7.pdf >.

II. Monitoring Compliance

Agencies providing HIV and AIDS services should develop, implement and systematically monitor compliance with confidentiality and data security policies. Policies should address staff/volunteer training, breaches in confidentiality, managing data (both within and outside of the agency), physical security, client privacy, release of client identifying information/records, electronic security (including faxes), telephone inquiries, discussions about clients, and penalties for violating client confidentiality. It is recommended that the agency develop written policies as well as provide routine quality assurance to verify that the policies meet the agency's standards.

III. Breaches in Confidentiality

All agency staff should report suspected security breaches of client confidentiality. A breach should be immediately investigated to assess causes and implement remedies consistent with the agency's policies. A breach that results in the release of private information about one or more individuals should be reported immediately to a supervisor, who should, in turn, report it to the health officer or agency director. In consultation with the appropriate legal counsel, staff should determine whether a breach warrants reporting to law enforcement agencies.

IV. Personnel and Training

It is recommended that agencies provide all new and existing employees with a copy of the agency's confidentiality policy. New employees, volunteers, and interns should receive training soon after being hired. Documentation of all staff training should be kept in agency operations/policy manuals in both the HIV/AIDS and the agency director's offices.

Every individual with access to HIV/AIDS client data should attend security and confidentiality training on a regular basis; several agencies provide training annually. All staff, including managers, maintenance employees, counseling and medical staff, as well as interns and the agency's authorized visitors (such as auditors and MDCH accreditation reviewers), should have limited access to HIV/AIDS data and have signed a confidentiality agreement, renewed annually, to abide by the agency's policies. Access to data should be determined on a need-to-know basis.

Confidentiality training should include:

- 1) Explanations of federal and state mandates for confidentiality upon which HIV/AIDS prevention and care services are based, and how infractions can result in harm to individuals as well as damage the confidence of the public in the agency's ability to provide services;
- 2) Review of Michigan's Public Health Code governing confidentiality of HIV/AIDS data and associated penalties for violation;
- 3) Review of confidentiality and client privacy safeguards, and the specific office procedures that must be followed. Examples should be discussed of ways to handle both routine and potentially compromising situations that may occur within the scope of each employee's duties. Each staff is responsible for protecting their own work area, including hardcopy and computer files containing HIV/AIDS client data. This responsibility includes protecting keys, passwords, and codes that allow access to confidential information. Staff must take care not to infect software with computer viruses. Screening interactions with clients about risk, possible STD infection, and other private matters must be conducted out of hearing range of other clients and staff. Counseling must be conducted in rooms where conversations cannot be heard in adjacent rooms, hallways, or from behind closed doors;
- 4) Giving a hardcopy of this policy to each new employee;

- 5) Written agreements signed by each employee pledging to maintain confidentiality in accordance with agency policy; the pledge should include information that employees/contract employees may be liable for criminal and civil penalties for such disclosures;
- 6) A written agreement declaring that there are no potential conflicts of interest related to this employment (sample attached in Appendix B);
- 7) All HIV staff are responsible for questioning unidentified visitors. HIV staff must also be responsible for reporting suspected security breaches;
- 8) Hardcopy documents containing confidential information should be shredded before disposing of them.

Employees, at the time of their resignation (or discharge), should sign a statement, including a detailed list, certifying they have returned all files, documents, office and file keys, identification badges, phone cards, laptops, cell phones, palm devices, and other equipment to the agency.

All employees leaving agency employment should be reminded that confidentiality extends indefinitely beyond the time that they leave employment, per state law.

V. Operations and Management of Confidential Data

Access to confidential materials (electronic and paper files) must be restricted to authorized staff on a need-to-know basis. Authorized staff are those whose job duties require access to client identifying information. For the purposes of this policy unauthorized persons are defined as visitors or any member of the agency or other staff (including housekeeping, administrative support, and building/maintenance staff) who do not have access to patient identifying information as a part of their work duties, as well as staff who do not work with HIV/AIDS clients.

All staff that are authorized to access client HIV/AIDS data should be responsible for questioning and challenging those who are not authorized if they attempt to access data.

VI. Physical Security

All staff authorized to access HIV client data are individually responsible for protecting their own workstation, laptop, or other devices associated with confidential information or data.

All computers are kept in locked rooms or suites with access limited to key HIV/AIDS prevention/care staff. Access to the offices by cleaning staff and maintenance/building staff is granted only during hours when authorized personnel are present or after all confidential materials are locked up and computer access is exited.

Detailed information on computer network security is in the HIV/AIDS Surveillance Program confidentiality guidelines, referenced on page 1.

VII. Client Privacy

As noted above, all screening, counseling, and discussions about HIV client risk activities and personal information must be conducted so that other clients in the agency are unable to hear conversations. It may be useful to provide “white noise” machines or radios played at low volume to mask staff-client discussions, whether in a counseling/exam room, lab/blood drawing area, or in the reception area. Of course, all clients should be reassured that their private and confidential information will be safeguarded with storage in locking file cabinets, locking offices and/or exam rooms, and in wings of the agency where clients and non-HIV staff have limited access, as reasonable and appropriate. Some agencies have erected privacy screens in reception areas to further mask staff-client interactions. Agencies are encouraged not to label areas, hallways, or doors with signs reading “AIDS,” “HIV,” “STD” or similar language that may compromise client confidentiality and privacy.

VIII. Securing Data Outside of Offices

Regardless of the strength of security practices in offices, confidential information transported outside of the office can easily become the weak link in the system. Carrying named client data out of the office requires specific supervisory approval and must be kept to a minimum.

Staff taking HIV client information into the field should consult the booklet, “Michigan HIV Laws: How They Affect Physicians and Other Health Care Providers – January 2006” (website address: < www.michigan.gov-documents-mihivlaws_49845_7.pdf >). Also please refer to the following key documents for further information:

Policy on Release of Data to Outside Agencies
MDCH HIV/AIDS Surveillance Office Procedure Manual

Copies of these may be obtained at the website: www.michigan.gov/hivstd.

IX. Handling Paper with Patient Identifying information/Lists

Confidential materials (including but not limited to case reports, and/or any paper with identifying information or lists of client names) must be handled with the utmost care. The amount and sensitivity of information in a single piece of mail must be kept to a minimum.

Mailing labels and stamped envelopes must **not** include the words “HIV or AIDS” or any similar reference. Whenever confidential information is mailed the envelope should be addressed to a

specific 'named' person and clearly marked as confidential.

NOTE: Absolutely NO lists should be maintained of HIV infected clients under any circumstances, as referenced in the state public health code.

Below are some common situations and ways to avoid compromising confidentiality with written materials. These serve as examples only and **are not** meant to be exhaustive.

1) Client charts/materials with identifying information (e.g., phone messages, forms, etc):

- a) Are kept in locked metal/steel file cabinets inside locked offices/suites and offices/suites that contain confidential material are locked whenever they are vacated during the day, even if it is for a short time period;
- b) Are shredded, ideally using a crosscut shredder, when they need to be discarded or disposed of;
- c) Are not taken to private residences unless specific documented permission is received by a supervisor or health officer. Each staff member will inform their supervisor upon request about how they handle visits at each off-site activity or program.

2) Faxing: Generally, fax machines used to send or receive HIV data should be kept in a secured area or room, beyond the view of clients. If it is not practical to utilize a secured room, then HIV data should not contain the patient's name or address or other identifying information. Identifying information should be communicated by telephone. Staff should be alerted when faxes are being sent to stand at the fax machine to receive fax. The sender will be instructed to use a full cover sheet with the name and phone number of the recipient clearly marked. It is recommended that the fax cover sheet include a confidentiality statement, similar to those included in MDCH e-mail communications (sample included in Appendix A). In all agencies, senders who are faxing confidential information should be given the number of the secure confidential fax machine and not the general fax machine.

3) Rooms with open access: When confidential materials are handled in a room with access (e.g., for copying) to aisles/hallways, they should be placed in a locked file when not in use and while being handled are kept out of view of unauthorized persons;

4) Staff work areas/"cubes": Confidential materials handled in private work areas should be kept from view of unauthorized persons. For example, client HIV charts and case report forms should **not** be left on a desktop when authorized staff persons are out of the office. Staff work areas should provide limited access to unauthorized persons, as well as to staff who do not have a need-to-know.

5) Conversations about clients: Such discussions should be carried on behind closed doors and never carried out in a space (e.g., offices or hallways) when unauthorized persons are present;

6) Cases or identifying information of potential cases are not discussed with anyone unless you know that the person already knows the patient's name and HIV/AIDS diagnosis:

- a) Do not disclose the name of a client living in one county with the local health department/CBO staff from another area unless the second agency's staff already know the client's name/diagnosis, or the client has signed a release for his/her medical information.
- b) Do not reveal the identifying information of suspect cases to health care providers unless there is clear evidence that that provider is treating or has treated the client.
- c) When in doubt, do not share client HIV medical information.

X. Answering Telephone Inquiries and Knowledge of HIV Infection Status

Staff should always know to whom they are talking. Never give information about whether a person is or is not HIV infected, or is in treatment at the agency, to someone over the phone unless staff are certain the other(s) are who they claim to be; this can not be overemphasized in importance. All agencies would benefit from development of a specific verification procedure.

Knowledge of someone's medical status (HIV or other HIV-related medical information) obtained in either a work or social setting during or after one's work with the program is to be treated confidentially, i.e., not shared with persons outside of the program or with co-workers unless they have the need-to-know because of their responsibilities.

Identifying information should not be left on voice mail. If staff need to use voice mail, an agency number can be left, but HIV/AIDS and the patient's identifying information will not be mentioned. Identifiable case follow-up information should not be left on external voice mail systems. Staff should never assume that telephone voice mail systems are secure.

XI. Electronic Security

All confidential data that resides on dedicated secure HIV/AIDS servers and confidential database files should not be copied to individual workstations, hard drives, diskettes, memory jump drives, PDA's, other hand-held devices, or CD's from the servers.

Patient identifiable information/data must not be routinely stored on a laptop. If such data are copied to laptop, software that encrypts data as it is being copied should be installed on the laptop before use.

Passwords should be protected, and changed frequently. Passwords should be created in ways that are not easily deciphered (e.g., combinations of letters, both upper and lower case, and numbers).

XII. Electronic Transmission of Data

Any data that contain patient names or individual identifying information and are transferred electronically should use encryption and be password protected. Electronic mail communications should include the confidentiality clause described in Appendix A.

Use of e-mail should be limited to internal communications between agency staff on site to update client HIV medical record/case information obtained in daily work. Client identifying information and the use of the terms HIV/AIDS must not be used. The subject line will say 'update' or some other non-descript phrase. E-mail addresses must be double checked before the message is sent.

XIII. HIV/AIDS Client Data Release

Information that could identify an HIV/AIDS client is released only according to the parameters described in the Michigan Public Health Code. For a summary of these requirements, please consult the booklet, Michigan HIV Laws: What Physicians and Other Health Care Providers Need to Know (2006).

Access to HIV client information for non-public health purposes, such as litigation, discovery, or court order, will be granted only to the extent required by law, and approved by the local health officer and/or agency legal counsel.

XIV. Penalties for Violation

Michigan Compiled Laws (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 HIV client data security policy can result in immediate dismissal. In addition, supervisors may deny access to the HIV client information at their discretion until necessary (legal) investigation occurs.

XV. Further Information/Contacts

Local health department and community based agency staff are encouraged to contact HASP with questions about surveillance protocols, at (517) 335-8165. More general HIV/AIDS questions about confidentiality and privacy policies may be directed to Bob Barrie, Quality Assurance Coordinator, HIV/AIDS Prevention & Intervention Section, in the Division of Health, Wellness & Disease Control. He may be reached at (517) 241-5934, or barrie@michigan.gov.

XVI. References:

1. Confidentiality and Data Security Policy, HIV/AIDS Surveillance Program/Communicable Disease Division, MDCH, June 1997.
2. Michigan HIV Laws: What Physicians and Other Health Care Providers Need to Know, MDCH, January 2006.
3. Technical Guidance for HIV/AIDS Surveillance Programs, Volume III, Security and Confidentiality Guidelines. Centers for Disease Control and Prevention and Council of State and Territorial Epidemiologists. Centers of Disease Control and Prevention, 2006.

XVII. Acknowledgements

The Division of Health, Wellness & Disease Control gratefully acknowledges the content and editing contributions of the following individuals: Debra Garcia Luna (MDCH), Cheryl Gildner (Ingham County Health Department), Garry Goza (MDCH), Jimena Loveluck (HIV/AIDS Resource Center), Barbara Murray (AIDS Partnership Michigan), Eve Mokotoff (MDCH), Liisa Randall (MDCH), Debra Szwejda (MDCH), Sue Tremonti (Macomb County Health Department); and Bob Barrie (MDCH).

Final edition: August 1, 2009

APPENDIX A

Sample Confidentiality Clause for Electronic Mail

“Notice: This message, including any attachments, is intended solely for the use of the named recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure or distribution of this communication(s) is expressly prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy any and all copies of the original message.

“Any interpretations or analysis contained in this e-mail or attachments represent the understanding and the opinions of the author, are based solely on the information provided to the author, and are intended to provide guidance to [your agency’s] staff, and do not represent a legal position or interpretation of [your agency].”

APPENDIX B

Sample Statement of Conflict of Interest

“The [agency] employee shall not represent or act as an agent for any private interests, whether for compensation or otherwise, in any transaction in which the agency has a direct and substantial interest and which could reasonably be expected to result in a conflict between the employee’s private interests and official agency responsibilities.”