

Missouri Department of Health and Senior Services

**Bureau of HIV, STD, and Hepatitis
Confidentiality and Security Manual**

June 2008

TABLE OF CONTENTS

Missouri Department of Health and Senior Services
BUREAU OF HIV, STD, AND HEPATITIS
CONFIDENTIALITY AND SECURITY MANUAL
June 2008

Preface

I. General Background and Assurances	1
A. Definitions	1
B. Legal Background	3
1. Federal Regulations	3
2. State Reporting Regulations	3
C. Confidentiality Assurances	5
1. Signing of Confidentiality Oath.....	5
2. Designation of ORPs and Responsibilities	5
3. Delineation of Surveillance Staff Responsibilities	7
4. Displaying of Employee Identification Badges	7
5. Administration of Performance Appraisals	7
6. Evaluation of Confidentiality/Security at HIV/AIDS Contractual Sites ..	8
7. Description of Penalties for Unauthorized Disclosure	8
8. Training for HIV/AIDS Confidentiality/Security	8
II. Physical Security	9
A. Building/Restricted Access Area Security.....	9
1. MDHSS/BHSH	9
2. SLCHD	9
3. KCHD	10
B. Office/Surveillance Unit Security.....	10
1. Retention of Hard Copy Files	10
2. Keys to Hard Copy Storage	10
III. Computer Security	11
A. Database Security	11
B. PC Workstation Security	11
IV. Data Confidentiality and Security	12
A. Release of Data to Non-HIV/AIDS Surveillance Staff	12
B. Transfer of Surveillance Data	16
1. Contractors	16
2. CDC	16
C. Authorized Statewide HIV/AIDS Surveillance Staff	17
D. Back-ups of HIV/AIDS Surveillance Data	17
E. Disposal of HIV/AIDS Surveillance Data	17
F. Photocopying/Printing of HIV/AIDS Surveillance Data	18

V. Rapid Communication	18
A. Electronic	18
1. E-mail	18
2. Facsimile.....	18
B. Mail.....	18
1. Incoming	18
2. Outgoing	18
C. Telephone.....	19
1. Incoming	19
2. Outgoing	19
VI. Field Activities	19
A. Confidential Materials Transported to the Field.....	19
1. Line-listings	19
2. Laptops.....	19
B. Transportation of Confidential Materials	20
C. Additional Field Security Protocols.....	20
VII. Procedures for Systematic Review of HIV/AIDS Security and Confidentiality Practices	20

Missouri Department of Health and Senior Services
BUREAU OF HIV, STD, AND HEPATITIS
CONFIDENTIALITY AND SECURITY MANUAL
REVISED JUNE 2008

PREFACE

Within the state of Missouri, Jefferson City is the administrative headquarters for all state surveillance activities. HIV/AIDS, sexually transmitted diseases (STD), and hepatitis surveillance units are located in Jefferson City. There are two additional HIV/AIDS specific surveillance units located in Kansas City and St. Louis. These three units are responsible for implementing and operating comprehensive HIV/AIDS surveillance programs to reduce the spread of HIV, STD, and hepatitis infection and their impact on at-risk populations. Surveillance program activities guide prevention policy decisions, target prevention resources, and assist in evaluating prevention and treatment activities. The surveillance units worked together to create this manual to provide guidelines for the management of confidential patient information to protect patient level information and to comply with state and federal statutes relating to patient confidentiality within state surveillance activities related to HIV/AIDS, STD, and hepatitis.

This manual serves as the official confidentiality security policy of the Missouri Department of Health and Senior Services (DHSS) that pertains to HIV/AIDS, STD, and hepatitis data. These policies encompass all agencies that contract with DHSS.

If you would like more information or statistics on the diseases discussed in this manual, please visit our website at <http://dhss.mo.gov> or call (573) 526-5271.

I. GENERAL BACKGROUND AND ASSURANCES

A. DEFINITIONS

1. **AIDS:** Acquired Immune Deficiency Syndrome.
2. **ARTEMIS:** The current state Perinatal Hepatitis B Case Management Database used in the case management of Pregnant Hepatitis B infected women, their newborns, and any household or sexual contacts for the purposes of ensuring immunoprophylaxis to those who are not immune.
2. **Bureau of HIV, STD, and Hepatitis (BHSH):** This organization performs statewide surveillance for HIV/AIDS, STD, and hepatitis and is located organizationally within the Division of Community and Public Health (DCPH), DHSS central office. The BHSH Surveillance Program is responsible for conducting and/or oversight of all statewide HIV/AIDS, STD, and hepatitis surveillance activities.
3. **Confidential Information/Material:** All HIV/AIDS, STD, and hepatitis information is inherently confidential and is considered as some of the most confidential

information managed by state and local health departments. Confidential information is considered as any information that could either directly (e.g., patient identifiers) or indirectly (e.g., small cell aggregate data) lead to the identification of a person reported with HIV/AIDS, STD, hepatitis, or any other person whose identity was learned through a case investigation, case report, personal interview, database, or research study.

4. **Contractor (Contractual Employees/Agreements):** Entities funded to perform HIV/AIDS, STD, or hepatitis case surveillance or case management through contractual agreements with DHSS. Current relationships exist with Kansas City Health Department (KCHD) , St. Louis City Department of Health and Hospitals (SLCHD) and St. Louis County Department of Health (SLCOHD).
5. **HBV:** Hepatitis B Virus
6. **HCV:** Hepatitis C Virus
7. **eHARS (Enhanced HIV/AIDS Reporting System):** National, statewide, and local database for conducting HIV/AIDS case surveillance.
8. **HIV:** Human Immunodeficiency Virus.
9. **Immediately:** With respect to reporting all breaches or suspected breaches of confidentiality [whether local health department to state health department or state health department to the Centers for Disease Control and Prevention (CDC)], immediately is defined as within the same working day. If an event occurs late in a working day, the statewide and/or local overall responsible parties are to be notified after normal working hours as soon as possible after the event occurs.
10. **MOHSIS (Missouri Health Surveillance Information System):** Statewide database for conducting hepatitis case surveillance.
11. **Overall Responsible Parties (ORPs):** Designated individuals at DHSS and local contractual sites who are ultimately responsible for the security and confidentiality of HIV/AIDS, STD, and hepatitis surveillance information.
12. **Security (Secured):** All measures implemented to prevent access to confidential material by unauthorized individuals as described in this document. Examples of security include physically secured facilities, restricted access areas, password-protected databases, and HIV/AIDS, STD, and hepatitis surveillance staff training.
13. **STD:** Sexually Transmitted Disease
14. **STD*MIS (Sexually Transmitted Disease Management Information System):** National and statewide database used for conducting STD case surveillance.

15. Unauthorized Release/Disclosure of HIV/AIDS, STD, and Hepatitis Surveillance Information: All release/disclosure of HIV/AIDS, STD, and hepatitis surveillance information not authorized by the ORP as defined in Section IV, paragraphs A and C of this manual.

B. LEGAL BACKGROUND FOR SECURITY/CONFIDENTIALITY OF HIV/AIDS AND HEPATITIS SURVEILLANCE INFORMATION

1. Federal Regulations. At the national level, eHARS is protected by the Federal Assurance of Confidentiality of Public Health Service Act, 42 U.S.C. 242k and 242m(d), that prohibits disclosure that could be used to directly and indirectly identify patients.

2. State Reporting Regulations. At the state level, multiple regulations dictate HIV/AIDS and hepatitis B and C reporting, security/confidentiality, and are described below:

a. Reportable Diseases and Conditions-19 CSR 20-20.020. The diseases, conditions, and findings that are reportable to the local health authority or DHSS are listed in this rule along with the designated time frames in which reporting must occur.

b. Physician Reporting-19 CSR 20-26.040. Physicians or their designees are required to report all conditions listed in 19 CSR 20-20.020 including HIV and hepatitis B and C. HIV infection is reportable as indicated by HIV antibody testing (reactive screening test followed by a positive confirmatory test), HIV antigen testing (reactive screening test followed by a positive confirmatory test), detection of HIV nucleic acid (RNA or DNA), HIV viral culture, or other testing which indicates HIV infection; newborn infants whose mothers are infected with HIV; HIV test results (including both positive and negative results) from children less than two years of age whose mothers are infected with HIV; AIDS; CD4 lymphocyte counts; and HIV viral load measurements. Providers are protected from any civil liability for reporting under RSMo. 191.656, Subsection 7. Hepatitis B, and C infections are indicated by positive antigen, antibody, and or DNA, RNA testing. Hepatitis B may be identified as a positive HBsAG, or HBeAG (antigen) test; a positive EIA – anti-HBc (Core Total) and anti-HBc, IgM, tests, confirmation tests such as the recombinant immunoblot assay (RIBA), or positive nucleic acid tests, and also by genotype testing. Hepatitis C may be identified by positive EIA Hepatitis C antibody tests, RIBA tests, and/or positive nucleic acid tests, and also by genotype testing.

c. Laboratory Reporting-19 CSR 20-20.080. Laboratories are required to report any positive test or any test indicative of conditions listed in 19 CSR 20-20.020 including the above tests for HIV infection, AIDS, CD4 lymphocyte counts, and viral load measurements. Laboratories are required to report any positive or any test indicative of hepatitis B or C.

- d. Exemptions to Reporting-19 CSR 20-26.040.** Exemptions from HIV/AIDS case reporting include: (1) all research institutions obtaining Institutional Review Board approval (IRB) for a specific study with notification of the board's approval submitted to DHSS in writing prior to commencement of study; or (2) where prohibited by federal law or regulation. There are no exemptions for reporting hepatitis B or C.
- e. State Statutes which Address Authorized Release of Surveillance Information.** Specific entities to which HIV/AIDS surveillance data can be released are described in Section IV, paragraphs A and C of this document.
- 1). **RSMo.167.183.1.** Immunization status for childhood diseases as required by RSMo.167.181 and 210.003 may be disclosed and exchanged without written consent to persons who have a direct business need to know such as public employees, school districts and child care facilities, persons who are entrusted to care for those under the care of state agencies, and health care professionals. (Attachment 1)
 - 2). **RSMo.191.656.** HIV/AIDS patient information can only be released to public employees with a need-to-know in order to perform their duties or private employees entrusted with patient care. Additional exceptions are outlined Subsection 2. (1) of RSMo.191.656 (Attachment 2).
 - 3). **RSMo.191.677.** This revised statute (Attachment 3) allows release of information by court order to allow for the prosecution of individuals who knowingly transmit HIV infection.
 - 4). **RSMo.191.658.** This revised statute (Attachment 3a) may allow release of HIV information (if on file) to a health care practitioner providing treatment for a health care worker or law enforcement officer because of a medically significant exposure to blood or body fluids.
- f. Penalties for Unauthorized Release of Surveillance Information.**
- 1). Penalties for unauthorized release of HIV/AIDS patient information are classified as (1) negligent violation and (2) willful, intentional, and reckless violation. Negligent violation can result in a fine of \$1,000, including all associated court costs and reasonable attorney's fees. This is in addition to other relief the court may judge appropriate. Willful violation can incur a fine of \$5,000, including exemplary damages, court costs and reasonable attorney's fees, in addition to other relief the court may deem appropriate.
 - 2). Breach of security and confidentiality pertaining to HIV/AIDS, STD, or hepatitis surveillance information may result in suspension, demotion, or termination based on the severity of the offense. Severity of offense and

disciplinary action for all DHSS staff with access to HIV/AIDS, STD, and hepatitis surveillance information is determined by the statewide ORP. Local health department administrators may elect to consult with DHSS administrators to determine the severity of offense and disciplinary action for employees of local contractual sites. The basis for disciplinary actions for DHSS staff is found in the DHSS Administrative Manual, Chapter 10, Section 10.4 (Attachment 4).

- 3). Penalties for contractual programs that breach confidentiality of HIV/AIDS, STD, or hepatitis surveillance information may include a reduction or loss of federal and/or state funding.

C. CONFIDENTIALITY ASSURANCES

1. Signing of Confidentiality Oath. All statewide surveillance staff and non-surveillance staff authorized to access HIV/AIDS, STD, and hepatitis surveillance information sign a DHSS confidentiality statement upon hire. In addition, all surveillance staff and other staff who have access to confidential data (e.g., STD Disease Intervention Specialists, Tuberculosis Control staff, designated information systems specialists in DHSS and in contractual sites) annually sign a confidentiality oath pertaining to HIV/AIDS, STD, and hepatitis surveillance information (Attachments 5, 6, 7, 8, and 9) and receive a confidentiality packet as described in paragraph 8 of this section. The signed (original) confidentiality statement is retained in the employee’s personnel file and a copy is given to the employee.

Figure 1. Confidentiality Assurances

- Confidentiality Oaths
- Overall Responsible Parties (ORPs) and Responsibilities
- Surveillance Staff Responsibilities
- Employee Identification Badges
- Performance Appraisals
- Contractual Staff
- Penalties for Unauthorized Disclosures
- Training

2. Designation of ORPs and Responsibilities. DHSS has identified statewide (Figure 2) and contractual (Figure 3) ORPs who are ultimately responsible for the confidentiality and security of HIV/AIDS, STD, and hepatitis surveillance information.

Figure 2. Statewide ORP

Statewide:
Mike Herbert, Chief
Bureau of HIV/STD/Hepatitis

Statewide ORP: Specific responsibilities of the statewide ORP include:

- a. Exercising the authority to make decisions about the overall HIV/AIDS, STD, and hepatitis surveillance operation that affect how surveillance information is collected, stored, analyzed, released, and disposed. Decisions also include which programs outside of HIV/AIDS, STD, and hepatitis surveillance are authorized to access surveillance data for public health purposes. This includes both DHSS central office and contractual sites.

- b. Collaborating closely with the Disease Surveillance Manager, HIV/AIDS Surveillance Coordinator, STD Program Manager and Viral Hepatitis Prevention Program Manager to annually certify that all CDC program requirements are met. Annually completing CDC’s certification form (Attachment 10).
- c. Collaborating closely with the Disease Surveillance Manager, HIV/AIDS Surveillance Coordinator and/or STD Program Manager and/or the Viral Hepatitis Prevention Program Manager to immediately report all breaches of confidentiality to the Reporting, Analysis, and Evaluation Team Leader, HIV Incidence and Case Surveillance Branch, CDC, and other relevant CDC Program Consultants.
- d. Collaborating with the HIV/AIDS Surveillance Coordinator, Disease Surveillance Manager, and Viral Hepatitis Prevention Program Manager to take appropriate disciplinary action toward central office surveillance staff and surveillance contractual entities that breach the confidentiality of HIV/AIDS, STD, or hepatitis surveillance information. The statewide ORP will also collaborate with managers of other DHSS programs whose employees breach confidentiality of HIV/AIDS, STD, or hepatitis surveillance information to establish appropriate disciplinary action.

State and local health department administrators will consult with their Department’s General Counsel to determine whether a breach warrants reporting to local and state law enforcement agencies.

Local ORPs:

Based on the fact that SLCHD and KCHD are contractual sites that use eHARS, STD*MIS and MOHSIS, DHSS is requesting that these health departments designate an individual to serve as the ORP for their respective surveillance jurisdictions (Figure 3). Local ORP responsibilities include:

Figure 3. Local ORPs

<p>SLCHD: Pamela Walker, MPA, Chief Bureau of Communicable Disease</p> <p>KCHD: Ron Griffin, MPH, Manager Division of Communicable Disease Prevention and Public Health Preparedness</p>
--

- a. Certifying annually that all CDC program requirements are met for their surveillance jurisdiction. Annually completing DHSS’s certification form (Attachments 11 and 12).
- b. Assuring ongoing jurisdiction adherence to all policies/procedures in Missouri’s *Bureau of HIV, STD, and Hepatitis Confidentiality and Security Manual*.
- c. Collaborating closely with the Disease Surveillance Manager, HIV/AIDS Surveillance Coordinator, STD Program Manager and Viral Hepatitis Prevention Program Coordinator to immediately report and resolve all breaches of confidentiality pertaining to HIV/AIDS, STD, and hepatitis surveillance data within their surveillance jurisdiction.

- d. Ensuring that all staff managing HIV/AIDS, STD, and hepatitis surveillance information are appropriately trained in all aspects of security and confidentiality.
- 3. Delineation of Surveillance Staff Responsibilities.** Surveillance staff have the following general responsibilities pertaining to the security and confidentiality of HIV/AIDS, STD, and hepatitis surveillance information:
- a. Releasing of data to non-HIV/AIDS, non-STD, and non-hepatitis surveillance staff is regulated by statements in Section IV, paragraph A of this manual.
 - b. Immediately reporting all suspected breaches of confidentiality to the statewide ORP or designee. DHSS central office surveillance staff should report all breaches or suspected breaches of confidentiality to the Disease Surveillance Manager, HIV/AIDS Surveillance Coordinator, STD Program Manager, Viral Hepatitis Prevention Program Manager or Chief, BSHS. Staff in local contractual sites should report all breaches or suspected breaches of confidentiality to their designated local ORP who will then immediately notify the statewide ORP or designee. All breaches of confidentiality are immediately reported to CDC and investigated to assess causes and implement remedies. In consultation with DHSS General Counsel, surveillance staff determine whether a breach warrants reporting to law enforcement agencies.
 - c. Exercising good judgment in the daily management of HIV/AIDS, STD, and hepatitis surveillance information. From time to time, confidentiality and security issues related to HIV/AIDS, STD, and hepatitis surveillance data may arise that are not specifically addressed in this manual. When these issues arise, surveillance staff are responsible for notifying the statewide ORP (or local ORP for contractual sites) who can provide the necessary guidance related to these issues.
 - d. Ensuring confidentiality of individual surveillance workstations.
Specific surveillance staff responsibilities pertaining to security/confidentiality of surveillance data are listed in the “Individual Office Security Checklist – HIV/AIDS, STD, and Hepatitis Surveillance” (Attachment 13).
- 4. Displaying of Employee Identification Badges.** HIV/AIDS, STD, and hepatitis surveillance staff statewide are required to display identification badges specific to their health department(s). These badges are required to be worn at all times when surveillance staff are working within the surveillance unit and also when conducting official activities away from the surveillance unit.
- 5. Administration of Performance Appraisals.** Confidentiality is listed as a job component on all BSHS and contractual staff performance appraisals.

6. **Evaluation of Confidentiality/Security at HIV/AIDS, STD and Hepatitis Contractual Sites.** Assurance of confidentiality is listed in annual surveillance contracts with the SLCHD and KCHD. The BSHS surveillance staff conduct biannual site visits with contractors to evaluate delivery of service, one area being confidentiality and security of HIV/AIDS, STD, and hepatitis surveillance information.
7. **Description of Penalties for Unauthorized Disclosure of HIV/AIDS, STD, and Hepatitis Surveillance Information.** Penalties for unauthorized disclosure of HIV/AIDS, STD, and hepatitis patient information are outlined in Section I, paragraph B2e of this manual.
8. **Training for HIV/AIDS, STD, and Hepatitis Confidentiality/Security**
 - a. **New Employee Orientation.** All new surveillance staff and non-surveillance staff authorized to access HIV/AIDS, STD, and hepatitis surveillance information are given a confidentiality orientation and are provided the following items:
 - *Bureau of HIV, STD, and Hepatitis Security and Confidentiality Manual*
 - DHSS Rules Pertaining to HIV/AIDS, STD, and hepatitis (including penalties for unauthorized disclosure)
 - “Individual Office Security Checklist – HIV/AIDS, STD, and Hepatitis Surveillance”
 - HIV/AIDS, STD, and Hepatitis Surveillance Program Confidentiality Statements

During the orientation, all new surveillance staff are thoroughly trained on the methodology of HIV/AIDS, STD, and hepatitis surveillance including protocols for HIV/AIDS, STD, and hepatitis security/confidentiality. Newly hired staff sign a confidentiality statement before access to surveillance data is authorized. This statement indicates that the employee understands and agrees that HIV/AIDS, STD, and hepatitis surveillance information or data will not be released to any individual not granted access by the ORP. Dates of security orientation are documented in each employee’s personnel file.

- b. **Annual Updates/Trainings.** Confidentiality updates/reviews are held annually during one of the statewide surveillance meetings. Updates allow for sharing of information regarding confidentiality/security including discussion of new policy, review of existing policy, review of CDC program requirements, discussion of areas of perceived weakness within the statewide program, and discussion of contractual and individual penalties for unauthorized disclosure of confidential information. All non-surveillance staff authorized to access surveillance information are also provided confidentiality and security training on an annual basis. This training includes the directive to report all suspected breaches of confidentiality. The date of training is documented in the employee’s personnel file.

- b. Other Trainings.** Surveillance staff statewide attend all CDC recommended or required confidentiality trainings.

II. PHYSICAL SECURITY

A. BUILDING/RESTRICTED ACCESS AREA SECURITY

Access to all restricted areas is limited to surveillance staff or other authorized individuals (e.g., program administrators, data managers) who have a need for access. Keys and/or electronic access cards are issued to surveillance staff upon hire and are surrendered to designated administrative staff upon either resignation or termination.

- 1. Bureau of HIV, STD, and Hepatitis (BHSB).** BHSB is located in one of three buildings operated by DHSS. Access to each building during normal business hours (defined as 6:30 am to 5:30 pm Monday through Friday) is through one entrance. All visitors are required to register at the front information desk and to display a visitor identification badge. BHSB (and thus the HIV/AIDS Surveillance Program, STD Surveillance Program and Hepatitis Surveillance Program) is located in a secure area on the north side of the building. This work area can be accessed through the front door that requires electronic access through two doors before reaching the unit. Once the unit is reached, electronic access is required to enter the unit. A sign is posted outside the door leading to the unit that indicates the unit's area is restricted. An exit door only is located within the unit. A combination is required to enter this door. Only authorized DHSS personnel have this combination. BHSB staff do not have this combination. BHSB staff must accompany visitors in order to enter the unit. Outside windows are secure. The HIV/AIDS Surveillance Coordinator and eHARS Database Administrator have offices with doors located in the back of the unit. Doors are kept closed during lunch and non-work hours. eHARS and other confidential databases are housed on a confidential fileserver located within the DHSS Information Technology Support Division (ITSD) area, not on individual workstations. ITSD is located in a separate building from the DCPH work area and the fileserver is located within an electronically secured room with limited numbers of information systems administrators granted security clearance to this room. All DHSS entrances in addition to the DCPH work area also require electronic access after hours and on weekends of which only a limited number of individuals have access. In the event that an access card is lost or stolen, it is immediately reported to the DCPH Deputy Director who is responsible for reporting the lost/stolen card to the security company.
- 2. St. Louis City Department of Health and Hospitals (SLCHD).** The HIV/AIDS surveillance unit is located within the Metropolitan St. Louis AIDS Program on the fourth floor of the SLCHD. Therefore, the unit is not accessible by windows. The surveillance unit is a restricted access area with double-locked doors. Both the building and the unit are locked after normal working hours (defined as 8:00 am to 5:00 pm, Monday through Friday). A security guard is posted in the building twenty-

four (24) hours a day and all authorized health department staff are required to sign-in for access after normal working hours. The surveillance unit is locked if no one is present within the unit. Cleaning crews do not access the surveillance unit after normal working hours.

- 3. Kansas City Health Department (KCHD).** The HIV/AIDS surveillance unit is located in the Communicable Disease Prevention Unit on the second floor of the KCHD. Building access is restricted with only one entrance open to the public. Security guards are posted in the health department while the building is open. The building has recording cameras inside and outside as well as motion detector indicators. A security station is located at both the public and employee entrances. . Electronic key cards control building access to staff. All outside windows are secure, and individual suites within the building are separately keyed. The Communicable Disease Prevention Unit is allotted its own suite specifically for Communicable Disease surveillance activities. It requires electronic key card access and only staff who work in surveillance or communicable disease supervisors are provided access. It is restricted to those staff only. Other staff from the Kansas City Health Department do not have access to the area. All entrances to the KCHD require electronic access after hours and on weekends of which only four (4) individuals from the Communicable Disease Prevention Unit have access.

B. OFFICE/SURVEILLANCE UNIT SECURITY

1. Retention of Hard Copy Files

- a.** All surveillance units retain hard copy files of HIV/AIDS, STD, and hepatitis surveillance information. All hard copy information is stored in double locked filing cabinets and is accessible only by HIV/AIDS, STD, or hepatitis surveillance staff. All original hard copy files are housed in locked filing cabinets at the DHSS central office in Jefferson City.
 - b.** Hard copy documents are concealed or locked up when employees are absent from individual workstations for even brief periods of time.
 - c.** When hard copy files are no longer required to be kept, the files are shredded by surveillance unit staff using a crosscut shredder.
- 2. Keys to Hard Copy Storage.** Designated staff in each surveillance unit retains the keys to hard copy storage. However, all surveillance staff are responsible for insuring security of their individual workstations, including appropriate storage of hard copy files.

III. COMPUTER SECURITY

A. DATABASE SECURITY

1. eHARS is the primary database for HIV/AIDS surveillance tracking, STD*MIS is used for STDs and MOHSIS is used for hepatitis. Other supplemental databases (e.g., death certificate, pending case, dBase 5.0) are internally designed and used for epidemiological tracking. Access to all databases is restricted to necessary surveillance personnel via password protection.
2. All surveillance units have information system specialists (data administrators) responsible for maintaining all network and database security and integrity. In the DHSS central office, these individuals are organizationally located within and outside of the surveillance unit. In St. Louis and Kansas City, these individuals are organizationally located outside of the surveillance unit (e.g. health department director's office).
3. All surveillance units possess different configurations for network security and are outlined in Figure 4; however, the eHARS database is not maintained on any individual workstation.

Figure 4. HIV/AIDS Surveillance Network Configuration by Surveillance Unit

DHSS:	Connected to DHSS LAN (network), DHSS Information Technology Support Division (ITSD) administers fileserver containing HIV/AIDS surveillance information. Surveillance utilizes trustee rights to confidential volume on fileserver.
--------------	--

B. PC WORKSTATION SECURITY

1. All surveillance staff are individually responsible for protecting his/her workstation, laptop, or other devices containing HIV/AIDS, STD, and hepatitis surveillance information. This includes protecting keys, passwords, and codes that would allow access to confidential information/data.
2. Terminals for all statewide HIV/AIDS, STD, and hepatitis surveillance staff are single password protected. Passwords in all surveillance jurisdictions are at least a minimum of five characters. On an established basis in each jurisdiction, users change passwords to insure database security. Access to confidential databases are restricted to necessary surveillance personnel via group access authority and network password protection.
3. All surveillance staff log off the network at the end of each day or when leaving the office for extended periods of time (defined as 2 hours or more). In the event a user fails to log out, networks at SLCHD, KCHD and DHSS automatically log off users after a specified time.

4. BSHH terminals utilize privacy screens due to workstation configurations.
5. At DHSS, retention of any confidential information (other than the information contained in eHARS) is maintained on secured drives. At KCHD, confidential information in addition to eHARS is stored in dBase (a major supplemental database). Secured drives are protected, and access is restricted to the user group. The data manager or designated information specialists of DHSS, SLCHD and KCHD also have access. Secured drives are not needed at SLCHD due to network configuration.
6. After the HIV/AIDS Surveillance Coordinator's, STD Surveillance Program Manager's, or Viral Hepatitis Prevention Program Manager's approval, DHSS ITSD staff erase confidential HIV/AIDS, STD, or hepatitis information from disks and the computer's hard drives prior to surplus with Norton's WipeInfo (Government Erase).
7. Anti-virus software is installed on all terminals at DHSS, SLCHD, and KCHD. Surveillance staff are responsible for reporting all computer viruses or suspected computer viruses to their designated information systems staff.
8. All surveillance system hardware (file servers) are located in areas that are adequately regulated with respect to temperature to avoid software/hardware damage.

IV. DATA CONFIDENTIALITY AND SECURITY

A. RELEASE OF DATA TO NON-HIV/AIDS, NON-STD, OR NON-HEPATITIS SURVEILLANCE STAFF

1. All data released are in accordance with RSMo.191.656, 191.677 and 191.658 that provide general guidelines for the release of HIV/AIDS surveillance information. This manual approved by the statewide ORP, lists specific protocols and policies for the release of HIV/AIDS, STD, and hepatitis surveillance information.
2. All surveillance staff are required to exercise discretion when releasing any surveillance data. Surveillance staff should consult with the local or statewide ORP (or designee) if they have questions pertaining to release of HIV/AIDS, STD, or hepatitis surveillance information.
3. All surveillance information pertaining to a specific HIV/AIDS case may be released to known, authorized providers (including infection control practitioners) directly involved in the health care of a patient.
4. All surveillance information may be released to authorized out-of-state surveillance staff for the tracking of a patient within their jurisdiction.

5. Confidential information may be released to other agencies within or outside DHSS who require such information to perform their job responsibilities (Figure 5).

Figure 5. Agencies in Missouri Obtaining Confidential HIV/AIDS Information

- STD Control Program
- TB program
- Medicaid Waiver Program
- HIV Case Management
- State and Local Prosecuting Agencies

a. Sexually Transmitted Disease Control Program.

In Missouri, HIV/AIDS surveillance data are linked with partner notification activities for STD including HIV. Designated surveillance staff provide in-state and local contractual Disease Intervention Specialists (DIS) with only the patient information (demographic, clinical, and risk) needed to perform an effective field investigation. Surveillance staff also share information with out-of-state STD Control programs for the same reason. The efforts of DIS identify contacts to known cases and, therefore, can potentially identify new cases of HIV infection. When required, DIS also has an integral role in resolving NIR (no-identified risk) investigations. Exchange of information between HIV/AIDS surveillance staff and DIS staff is bilateral and occurs on both the state and local levels.

b. Tuberculosis Control Program. On a quarterly basis, in the DHSS central office, names and dates of birth of all tuberculosis infection, tuberculosis disease and mycobacterium other than tuberculosis (MOTT) cases are matched electronically to names and dates of birth of cases in eHARS. Designated HIV/AIDS surveillance staff conduct the match. If an individual has dual diagnoses (i.e., TB/MOTT and/or HIV/AIDS), the diagnosis and RVCT number is noted on the patient record in both the tuberculosis and eHARS registries. Hardcopy HIV/AIDS case reports are not shared with the tuberculosis program staff.

The KCHD HIV/AIDS Surveillance Program obtains names, dates of birth, and diagnosis of persons with tuberculosis disease or MOTT from the local tuberculosis program. After eHARS is record searched and the appropriate co-morbidity updated in eHARS, the tuberculosis program is then notified of the dual diagnosis of either HIV or AIDS. The tuberculosis program uses a numerical code to indicate those persons with co-morbidity (a three digit number which is used in place of the words “HIV or AIDS”).

The SLCHD HIV/AIDS Surveillance Program does not receive any information from their local tuberculosis program. Tuberculosis disease and MOTT updates are received on hardcopy from Jefferson City. This information is shredded after local entry into eHARS.

c. Missouri Medicaid Waiver Program. Upon request, designated HIV/AIDS surveillance staff confirm the HIV diagnosis of individuals receiving services under the Medicaid Waiver Program and report the status to designated Medicaid Waiver staff. Only confirmation of either HIV/AIDS diagnosis is provided to

Medicaid waiver staff, no additional surveillance information is provided. Medicaid information can also be a potential case finding/validation source for the Missouri surveillance program. Release of this information only occurs on the state level.

- d. HIV Case Management Program.** Upon request, HIV/AIDS surveillance staff verify the diagnosis of individuals who apply for Missouri HIV case management services. Case management links HIV diagnosed clients to care, community resources, and information. Confirmation of HIV/AIDS diagnosis (including appropriate laboratory information, CD4 counts, viral loads, and opportunistic infections) is provided to designated case management staff. Additional surveillance information (e.g., partner notification activity) may be provided if requested to assist with comprehensive patient management. Case management is also a valuable case finding/validation source for the Missouri surveillance program. Release of this information occurs on both state and local levels.
 - e. State and Local Prosecuting Agencies.** Upon request, HIV/AIDS surveillance information can be released to state and local prosecuting attorneys to enforce RSMo. 191.677. Release is coordinated by the Chief, BSHS along with DHSS General Counsel. The only information released to prosecutors is laboratory history to verify the status of the prosecuted individual. Release of information occurs only on the state level.
 - f. Perinatal Hepatitis B Case Management Program.** The Perinatal Hepatitis B Case Managers verify the diagnosis of every hepatitis B infected woman in Missouri in order to identify their babies and household and sexual partners for the purposes of providing appropriate immunoprophylaxis against hepatitis B. These case managers are employees of the state or local health departments charged with following these cases. Maternal and contacts' hepatitis B laboratory information are shared between state and local communicable disease staff responsible for these cases. These case workers must communicate with the health care providers who are responsible for the care of a baby born to a hepatitis B infected woman to provide necessary treatment within hours of birth. Additional surveillance information (e.g., partner notification activity) may be provided if requested to assist with comprehensive patient management. Case management is also a valuable case finding/validation source for the Missouri surveillance program. Release of this information occurs on both state and local levels.
- 6.** DHSS does not release HIV/AIDS surveillance information to law enforcement officials (e.g., defense attorneys, prosecuting attorneys, and detectives) not described under the scope of RSMo. 191.677 without a subpoena or court order, depending on the exact nature of the request. The statewide ORP or designee collaborates closely with the DHSS Chief Counsel to respond to all named-identifier requests from law enforcement. DHSS Chief Counsel collaborates with the State's Attorney General's Office to resist all such release of HIV/AIDS surveillance information. Local

contractual agencies are required to refer all requests from law enforcement to the statewide ORP or designee.

7. According to state statute, RSMo. 191.658, a health care practitioner, providing medical treatment for a health care worker or law enforcement officer because of a medically significant exposure to blood or other body fluids that occurred in the course of the worker's or officer's employment, may request from the DHSS, information regarding the HIV infection status of the source individual.

A protocol has been established for operationalizing the requirements of this statute and to reduce to a minimum the number of times the state registry is used to determine the status of a source individual. Local contractual agencies and central office staff are required to refer all requests from providers to the statewide ORP or designee. These requests are then routed to one of the designated state HIV consultants (e.g., consultant community health nurse, medical epidemiologist) who will determine if a significant exposure, as defined in the law, has occurred and if HIV information on the source individual is essential in providing necessary medical treatment. The caller will be provided with appropriate treatment recommendations and other medical information (e.g., assure the exposed individual is evaluated for hepatitis B and C as well as HIV, referring to CDC recommendations for post-exposure prophylaxis).

If the information collected meets the criteria set forth in the law and it is determined that the source person's HIV status is needed in order to determine or encourage ongoing appropriate treatment for the exposed individual, information on the exposed individual will be obtained (e.g., name, date of birth, race). This information will be referred to authorized surveillance staff in BSHS who have access to the eHARS database (Section C., Figure 4). Only those individuals with access to the eHARS database will know if the source patient is infected with HIV and will have the responsibility to notify the provider of the results.

8. State statute (RSMo. 191.689) requires school notification of children with HIV infection, only after a school has adopted a policy consistent with recommendations of CDC on school children that test positive for HIV. In view of concerns related to patient confidentiality, the HIV/AIDS surveillance program does not operationalize the statute.
9. Named HIV data are not released to researchers unless they sign the DHSS HIV/AIDS Surveillance Program confidentiality statement and are conducting a DHSS Institutional Review Board (IRB) approved project.
10. De-identified HIV/AIDS, STD, and hepatitis surveillance data sets are provided to statewide and local epidemiologists for the analysis of HIV/AIDS, STD, and hepatitis surveillance data.

11. The statewide HIV/AIDS, STD, and Hepatitis Surveillance Programs exercises great caution in public release of numerical, small cell data that could either directly or indirectly lead to the identification with a person infected with HIV/AIDS, STD, or hepatitis. Several independent variables (e.g., risk factor, race, age) could lead to the direct/indirect identification of a person with HIV/AIDS, STD, and hepatitis and should be carefully evaluated in view of the total population of the jurisdiction under observation including racial and risk distribution/prevalence. For the central office program, no small cell data are released without consent from the HIV/AIDS Surveillance Coordinator, STD Program Manager, Viral Hepatitis Prevention Program Manager, and/or Chief, BSHH. In contractual sites, no small cell data are released without the consent of the local ORP or designee.

B. TRANSFER OF SURVEILLANCE DATA

1. **Contractors.** HIV/AIDS surveillance contractual sites monthly transfer completed HIV/AIDS case forms and other confidential information to BSHH. Transfer is performed by hardcopy. Both contractual sites mail all hard copy data (i.e., completed HIV/AIDS case report forms, laboratory results) in double envelopes via certified mail. BSHH mails all confidential hard copy information to contractors in double envelopes sent via certified mail.

The Perinatal Hepatitis B Case Managers have access to MOHSIS and ARTEMIS by password protected entry. All other departmental security and encryption applications as afforded to other confidential material as described within this document apply.

2. **CDC.** BSHH encrypts all new and updated entries on eHARS records using SEAL encryption software. The files are then transmitted monthly to CDC through the Secure Data Network (SDN).

C. AUTHORIZED STATEWIDE HIV/AIDS SURVEILLANCE STAFF WITH ACCESS TO EHARS

Only authorized staff performing HIV/AIDS surveillance responsibilities have **direct** access to eHARS. Authorized surveillance staff for all three units and defined functions within that unit are listed in Figure 6.

Figure 6. Statewide Personnel* with Authorized Access to eHARS and Function

DCPH	Two HIV/AIDS Surveillance Research Analysts (HIV/AIDS Data Analysis) HIV/AIDS Database Manager (Statewide QA, Entry of Outstate Case Reports, Preparation of Statistical Reports) One Support Staff (Data Entry) HIV/AIDS Provider Specialist (Contacts providers to obtain information regarding lab and/or case reports received, Entry of Outstate Case Reports) STD Database Manager (eHARS Back up) Two STD Program Coordinators (Assistance to DIS Activities)
St. Louis City	HIV/AIDS Surveillance Coordinator (Preparation of Statistical Reports) HIV/AIDS Surveillance Specialist (City/County Core Surveillance) HIV/AIDS Surveillance Support (Data Entry)
Kansas City	HIV/AIDS Surveillance Coordinator (HIV/AIDS Case Surveillance, Preparation of Statistical Reports) Two Support Staff (Data Entry)

* Systems administrators in all three areas have access to eHARS for fileserver maintenance, but eHARS is not accessed on a routine basis.

D. BACK UPS OF HIV/AIDS SURVEILLANCE DATA

At DHSS, ITSD completes a full back up of all computer volume for DHSS users once a week, with incremental back ups daily. Data are saved on tapes that are stored in a locked room within the ITSD unit. Incremental back ups are kept for one week, full back ups are kept for one month; the last full back up on the last day of the month is kept indefinitely in an offsite safe to which only two ITSD system administrators have access.

E. DISPOSAL OF HIV/AIDS, STD AND HEPATITIS SURVEILLANCE DATA

1. All hard copy confidential information (e.g., CD4-lymphocyte, viral load reports, notes from medical record reviews, case reports, laboratory reports, field investigation paperwork) is shredded when no longer needed. For this purpose, the commercial quality shredders with a crosscutting feature are used.
2. All disks and computer hard drives are erased prior to surplus with Norton's WipeInfo (Government Erase).

F. PHOTOCOPYING/PRINTING OF HIV/AIDS, STD, AND HEPATITIS SURVEILLANCE DATA

Confidential information is not left unattended in common access areas and is retrieved immediately upon copying/printing.

V. RAPID COMMUNICATION

A. ELECTRONIC

- 1. E-Mail.** WinZip 9.0 (128-bit encryption capability) with password protection is used to send identifying information from BSHS to other DHSS staff and contractors.
- 2. Facsimile.** Dedicated facsimile (fax) lines are used to transmit confidential information between contractors, local public health communicable disease investigators and DHSS. Both contractual sites (KCHD, SLCHD) and DHSS have dedicated facsimile lines. Only authorized staff have access to the referenced fax machines. When authorized staff fax confidential information, the addressee is contacted prior to transmission via phone. Neither the cover sheet nor faxed material has any direct or indirect reference to HIV/AIDS. The confirmation of receipt should be sent from addressee to sender. The addressee should contact the sender if incoming faxes are not received within the expected timeframe. Hepatitis B laboratory reports and Perinatal Hepatitis B case management forms are specifically addressed to the LPHA Communicable Disease Nurse and sent to the designated fax machine for confidential information.

B. MAIL

- 1. Incoming-** Mailroom personnel are required to sign the DHSS confidentiality statement (Attachment 14) that covers all aspects connected with the confidentiality and security of communicable diseases in Missouri including HIV/AIDS, STD, and hepatitis. The mail is then dispersed to designated HIV/AIDS, STD, and hepatitis surveillance staff. Senders of confidential information are instructed to address mail to the designated surveillance unit. Physicians and other case reporters are provided return envelopes stamped “confidential” for submitting case reports. The return envelopes have no direct reference to HIV/AIDS. Appropriate administrative personnel (e.g., Program Manager at KCHD and HIV/AIDS Surveillance Coordinators at SLCHD and BSHS) shall be notified of all mail routed to the incorrect health department program and appropriate health department staff and/or providers notified to prevent reoccurrence.
- 2. Outgoing-** All outgoing mail containing patient identifiers is marked “confidential”, double enveloped, and sent via certified mail. No outgoing envelopes have any direct or indirect reference to HIV/AIDS. All outgoing hepatitis and STD related mail containing patient identifiers are sealed, taped and marked “confidential” and are sent

in manila Department of Health and Senior Services envelopes in which inside information cannot be seen from the outside.

C. TELEPHONE

- 1. Incoming-** Generic identifiers (e.g., “Department of Health and Senior Services”, “This is Joe”, “Section for Disease Control and Environmental Epidemiology”), without any direct reference to HIV/AIDS, STD, or hepatitis are used when answering all incoming calls. Confidential information is shared over the phone with individuals authorized to access HIV/AIDS, STD, and hepatitis surveillance information as listed in Section IV, paragraphs A and C. Specific techniques (e.g., call back verification) are recommended to determine authorized individuals.
- 2. Outgoing-** Confidential information is requested via phone to perform routine HIV/AIDS, STD, and hepatitis surveillance activities. Messages with identifying patient identifiers are not left on voice mail systems unless there is prior confirmation of a secure line. Staff discuss confidential information only in secure areas, release information to only those individuals with a need-to-know (as defined in Section IV, paragraphs A and C), and always use utmost discretion.

VI. FIELD ACTIVITIES

A. CONFIDENTIAL MATERIALS TRANSPORTED TO THE FIELD

1. Line listings

- a.** Line listings are routinely carried into the field to perform routine HIV/AIDS, STD and hepatitis surveillance activities.
- b.** Surveillance information on line listings is de-identified. Although line listings typically contain the patient name, date of birth, status (HIV or AIDS, diagnosis), and risk information, the status and risk information is coded either alphabetically or numerically (such as the coding system used in eHARS) so as to neither directly nor indirectly identify the contents of the line list.
- c.** Only patient information on work to be performed for that day is transported into the field.

Laptops. Laptops and other portable devices (PDA and other hand-held devices) that receive or store surveillance information with personal identifiers must use encryption software that meets the 128-bit encryption standard. When the laptops and portable devices are not in use, surveillance information with identifiers must be encrypted and stored on an external storage device or on the laptop’s removable hard drive. The removable media must include only the minimum amount of information necessary to

accomplish assigned tasks as determined by the HIV/AIDS Surveillance Coordinator, STD Program Manager, or Viral Hepatitis Prevention Program Manager; be separated from laptop and held securely when not in use; and be sanitized immediately following a given task (the exceptions are devices used for backups). Before taking any device containing sensitive data out of the secured area, the data must be encrypted. The decryption key must not be on the laptop. Other portable devices without removable or external storage components must employ the use of 128-bit encryption software.

B. TRANSPORTATION OF CONFIDENTIAL MATERIALS

1. All confidential materials are carried in a secured briefcase when performing field activities. Briefcases are never left unattended including in locked vehicles.
2. Confidential information should always be returned to the HIV/AIDS, STD, and hepatitis surveillance unit at the close of each business day. Prior approval must be obtained from the HIV/AIDS Surveillance Coordinator, STD Program Manager, or Viral Hepatitis Prevention Program Manager when out-of-town travel or some other reason precludes the return of confidential information to the unit.
3. When it is absolutely not possible to return confidential materials to the surveillance unit at the close of each business day (either because out-of-town travel, emergency, or for some other reason), confidential information is always stored in appropriate places (e.g., locked hotel rooms, private residences).

C. ADDITIONAL FIELD SECURITY PROTOCOLS

1. Surveillance staff always present health department identification when performing surveillance field activities.
2. All discussions pertaining to confidential information are conducted in secure, private areas. Medical record reviews are conducted as discreetly as possible.
3. Confidential information is never left in public or general access areas.

VII. PROCEDURES FOR SYSTEMATIC REVIEW OF HIV/AIDS, STD AND HEPATITIS SECURITY AND CONFIDENTIALITY PRACTICES

- A. The manual will be reviewed and updated accordingly on an annual basis.
- B. When all changes to information systems technology are proposed (e.g., fileserver configuration changes, purchase of new equipment for CDC pilot projects), information system specialists in all surveillance units are responsible for collaborating with the HIV/AIDS Surveillance Coordinator, STD Program Manager and Viral Hepatitis

Prevention Manager to prepare technical solutions. This collaboration will help ensure that in no way the security and confidentiality of HIV/AIDS, STD and Hepatitis surveillance data are electronically compromised.

Missouri Department of Health and Senior Services

Attachments

Missouri Revised Statutes

Chapter 167 **Pupils and Special Services** **Section 167.183**

August 28, 2007

Immunization records, disclosure, to whom--disclosure for unauthorized purpose, liability.

167.183. 1. Information and records pertaining to the immunization status of persons against childhood diseases as required by section 167.181 and section 210.003, RSMo, may be disclosed and exchanged without a parent's or guardian's written release authorizing such disclosure, to the following, who need to know such information to assure compliance with state statutes or to achieve age-appropriate immunization status for children:

- (1) Employees of public agencies, departments and political subdivisions;
- (2) Health records staff of school districts and child care facilities;
- (3) Persons other than public employees who are entrusted with the regular care of those under the care and custody of a state agency including, but not limited to, operators of day care facilities, group homes, residential care facilities and adoptive or foster parents;
- (4) Health care professionals.

2. If any person, authorized in subsection 1 of this section, discloses such information for any other purpose, it is an unauthorized release of confidential information and the person shall be liable for civil damages.

(L. 1992 S.B. 611)

Effective 7-6-92

[© Copyright](#)

Missouri Revised Statute

Chapter 191
Health and Welfare
Section 191.656

August 28, 2003

Confidentiality of reports and records, exceptions--violation, civil action for injunction, damages, costs and attorney fees--health care provider participating in judicial proceeding, immune from civil liability.

191.656. 1. (1) All information known to, and records containing any information held or maintained by, any person, or by any agency, department, or political subdivision of the state concerning an individual's HIV infection status or the results of any individual's HIV testing shall be strictly confidential and shall not be disclosed except to:

(a) Public employees within the agency, department, or political subdivision who need to know to perform their public duties;

(b) Public employees of other agencies, departments, or political subdivisions who need to know to perform their public duties;

(c) Peace officers, as defined in section 590.100, RSMo, the attorney general or any assistant attorneys general acting on his or her behalf, as defined in chapter 27, RSMo, and prosecuting attorneys or circuit attorneys as defined in chapter 56, RSMo, and pursuant to section 191.657;

(d) Prosecuting attorneys or circuit attorneys as defined in chapter 56, RSMo, to prosecute cases pursuant to section 191.677 or 567.020, RSMo. Prosecuting attorneys or circuit attorneys may obtain from the department of health and senior services the contact information and test results of individuals with whom the HIV-infected individual has had sexual intercourse or deviate sexual intercourse. Any prosecuting attorney or circuit attorney who receives

information from the department of health and senior services pursuant to the provisions of this section shall use such information only for investigative and prosecutorial purposes and such information shall be considered strictly confidential and shall only be released as authorized by this section;

(e) *Persons other than public employees who are entrusted* with the regular care of those under the care and custody of a state agency, including but not limited to operators of day care facilities, group homes, residential care facilities and adoptive or foster parents;

(f) As authorized by subsection 2 of this section;

(g) Victims of any sexual offense defined in chapter 566, RSMo, which includes sexual intercourse or deviate sexual intercourse, as an element of the crime or to a victim of a section 566.135, RSMo, offense, in which the court, for good cause shown, orders the defendant to be tested for HIV, hepatitis B, hepatitis C, syphilis, gonorrhea, or chlamydia, once the charge is filed. Prosecuting attorneys or circuit attorneys, or the department of health and senior services may release information to such victims;

(h) Any individual who has tested positive or false positive to HIV, hepatitis B, hepatitis C, syphilis, gonorrhea, or chlamydia, may request copies of any and all test results relating to said infections.

(2) Further disclosure by public employees shall be governed by subsections 2 and 3 of this section;

(3) Disclosure by a public employee or any other person in violation of this section may be subject to civil actions brought under subsection 6 of this

Attachment 2 (con't)

section, unless otherwise required by chapter 330, 332, 334, or 335, RSMo, pursuant to discipline taken by a state licensing board.

2. (1) Unless the person acted in bad faith or with conscious disregard, no person shall be liable for violating any duty or right of confidentiality established by law for disclosing the results of an individual's HIV testing:

- (a) To the department of health and senior services;
- (b) To health care personnel working directly with the infected individual who have a reasonable need to know the results for the purpose of providing direct patient health care;
- (c) Pursuant to the written authorization of the subject of the test result or results;
- (d) To the spouse of the subject of the test result or results;
- (e) To the subject of the test result or results;
- (f) To the parent or legal guardian or custodian of the subject of the testing, if he is an unemancipated minor;
- (g) To the victim of any sexual offense defined in chapter 566, RSMo, which includes sexual intercourse or deviate sexual intercourse, as an element of the crime or to a victim of a section 566.135, RSMo, offense, in which the court, for good cause shown, orders the defendant to be tested for HIV, B, hepatitis C, syphilis, gonorrhea, or chlamydia, once the charge is filed;
- (h) To employees of a state licensing board in the execution of their duties under chapter 330, 332, 334, or 335, RSMo, pursuant to discipline taken by a state licensing board;

The department of health and senior services and its employees shall not be held liable for disclosing an HIV-infected person's HIV status to individuals with whom that person had sexual intercourse or deviate sexual intercourse;

(2) Paragraphs (b) and (d) of subdivision (1) of this subsection shall not be construed in any court to

impose any duty on a person to disclose the results of an individual's HIV testing to a spouse or health care professional or other potentially exposed person, parent or guardian;

(3) No person to whom the results of an individual's HIV testing has been disclosed pursuant to paragraphs (b) and (c) of subdivision (1) of this subsection shall further disclose such results; except that prosecuting attorneys or circuit attorneys may disclose such information to defense attorneys defending actions pursuant to section 191.677 or 567.020, RSMo, under the rules of discovery, or jurors or court personnel hearing cases pursuant to section 191.677 or 567.020, RSMo. Such information shall not be used or disclosed for any other purpose;

(4) When the results of HIV testing, disclosed pursuant to paragraph (b) of subdivision (1) of this subsection, are included in the medical record of the patient who is subject to the test, the inclusion is not a disclosure for purposes of such paragraph so long as such medical record is afforded the same confidentiality protection afforded other medical records.

3. All communications between the subject of HIV testing and a physician, hospital, or other person authorized by the department of health and senior services who performs or conducts HIV sampling shall be privileged communications.

4. The identity of any individual participating in a research project approved by an institutional review board shall not be reported to the department of health and senior services by the physician conducting the research project.

5. The subject of HIV testing who is found to have HIV infection and is aware of his or her HIV status shall disclose such information to any health care professional from whom such person receives health care services. Said notification shall be made prior to receiving services from such health care professional if the HIV-infected person is medically capable of conveying that information or as soon as he or she becomes capable of conveying that information.

6. Any individual aggrieved by a violation of this section or regulations promulgated by the department of health and senior services may bring a civil action for damages. If it is found in a civil action that:

Attachment 2 (con't)

(1) A person has negligently violated this section, the person is liable, for each violation, for:

(a) The greater of actual damages or liquidated damages of one thousand dollars; and

(b) Court costs and reasonable attorney's fees incurred by the person bringing the action; and

(c) Such other relief, including injunctive relief, as the court may deem appropriate; or

(2) A person has willfully or intentionally or recklessly violated this section, the person is liable, for each violation, for:

(a) The greater of actual damages or liquidated damages of five thousand dollars; and

(b) Exemplary damages; and

(L. 1988 H.B. 1151 & 1044 § 3, A.L. 1992 S.B. 511 & 556 merged with S.B. 638, A.L. 1993 S.B. 233, A.L. 1996 S.B. 858, A.L. 1999 H.B. 191, A.L. 2002 H.B. 1756)

... These words appear twice in original rolls.

(1998) Prosecutors, judges and juries are public employees with a need to know for prosecutions pursuant to section 191.677. State v. Mahan, 971 S.W.2d 307 (Mo.banc).

(c) Court costs and reasonable attorney's fees incurred by the person bringing the action; and

(d) Such other relief, including injunctive relief, as the court may deem appropriate.

7. No civil liability shall accrue to any health care provider as a result of making a good faith report to the department of health and senior services about a person reasonably believed to be infected with HIV, or cooperating in good faith with the department in an investigation determining whether a court order directing an individual to undergo HIV testing will be sought, or in participating in good faith in any judicial proceeding resulting from such a report or investigations; and any person making such a report, or cooperating with such an investigation or participating in such a judicial proceeding, shall be immune from civil liability as a result of such actions so long as taken in good faith.



Missouri Revised Statute

Chapter 191 Health and Welfare Section 191.677

August 28, 2003

Prohibited acts, criminal penalties.

191.677. 1. It shall be unlawful for any individual knowingly infected with HIV to:

- (1) Be or attempt to be a blood, blood products, organ, sperm or tissue donor except as deemed necessary for medical research;
- (2) Act in a reckless manner by exposing another person to HIV without the knowledge and consent of that person to be exposed to HIV, in one of the following manners:
 - (a) Through contact with blood, semen or vaginal secretions in the course of oral, anal or vaginal sexual intercourse; or
 - (b) By the sharing of needles; or
 - (c) By biting another person or purposely acting in any other manner which causes the HIV-infected person's semen, vaginal secretions, or blood to come into contact with the mucous membranes or nonintact skin of another person.

Evidence that a person has acted recklessly in creating a risk of infecting another individual with HIV shall include, but is not limited to, the following:

- a. The HIV-infected person knew of such infection before engaging in sexual activity with another person, sharing needles with another person, biting another person, or purposely causing his or her semen, vaginal secretions, or blood to come into contact with the mucous membranes or nonintact skin of another person, and such other person is unaware

of the HIV-infected person's condition or does not consent to contact with blood, semen or vaginal fluid in the course of such activities;

b. The HIV-infected person has subsequently been infected with and tested positive to primary and secondary syphilis, or gonorrhea, or chlamydia; or

c. Another person provides evidence of sexual contact with the HIV- infected person after a diagnosis of an HIV status.

2. Violation of the provisions of subdivision (1) or (2) of subsection 1 of this section is a class B felony unless the victim contracts HIV from the contact in which case it is a class A felony.

3. The department of health and senior services or local law enforcement agency, victim or others may file a complaint with the prosecuting attorney or circuit attorney of a court of competent jurisdiction alleging that a person has violated a provision of subsection 1 of this section. The department of health and senior services shall assist the prosecutor or circuit attorney in preparing such case, and upon request, turn over to peace officers, police officers, the prosecuting attorney or circuit attorney, or the attorney general records concerning that person's HIV-infected status, testing information, counseling received, and the identity and available contact information for individuals with whom that person had sexual intercourse or deviate sexual intercourse and those individuals' test results.

4. The use of condoms is not a defense to a violation of paragraph (a) of subdivision (2) of subsection 1 of this section.

Missouri Revised Statutes

**Chapter 191
Health and Welfare
Section 191.658**

August 28, 2005

HIV infection status disclosure by department of health and senior services to exposed health workers or law enforcement officers, when, violation, penalty.

191.658. 1. As used in this section, the following terms shall mean:

(1) "Disclose", to disclose, release, transfer, disseminate or otherwise communicate all or any part of any record orally, in writing or by electronic means to any person or entity;

(2) "Health care practitioner", any licensed physician, nurse practitioner or physician's assistant;

(3) "HIV", the human immunodeficiency virus that causes acquired immunodeficiency syndrome;

(4) "HIV infection", the pathological state of the human body in response to HIV;

(5) "Medically significant exposure", a puncture through or laceration of the skin, or contact of mucous membrane or nonintact skin with blood, tissue, wound exudate or other body fluids, including semen, vaginal secretions, cerebrospinal fluid, synovial fluid, pleural fluid, peritoneal fluid, pericardial fluid, amniotic fluid or any body fluid containing visible blood, or contact of intact skin with any such body fluids when the duration of contact is prolonged or involves an extensive area of skin;

(6) "Person", private individuals, private or public bodies politic, and corporations, partnerships, trusts, and unincorporated

associations and their officers, directors, agents or employees;

(7) "Source individual", the person who is the source of the blood or other body fluids to which medically significant exposure occurred.

2. A health care practitioner providing medical treatment for a health care worker or law enforcement officer because of a medically significant exposure to blood or other body fluids that occurred in the course of the worker's or officer's employment may request from the department of health and senior services information regarding the HIV infection status of the source individual. The department of health and senior services may disclose to the health care practitioner the HIV infection status of the source individual if such information is on file with the department.

3. The health care practitioner shall disclose the HIV infection status of the source individual to the exposed health care worker or law enforcement officer if, in the professional judgment of the health care practitioner, such disclosure is necessary to assure adherence to a prescribed treatment regimen.

4. No person to whom information about an individual's HIV infection has been disclosed pursuant to this section shall further disclose such results.

5. Any person who knowingly releases information in violation of this section is guilty of a class A misdemeanor.

(L. 1999 H.B. 271 § 1)



ADMINISTRATIVE MANUAL

SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action	<i>Chapter:</i> 10
	<i>Section:</i> 10.4
REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070 RSMo 36.410 and 105.262	<i>Page:</i> 1 of 6
	<i>Revised:</i> 2-17-04

DISCIPLINARY ACTION

I. PURPOSE:

To set forth causes for disciplinary action, including suspension, demotion or dismissal, depending upon the seriousness of the violation. However, discipline may be based upon causes other than these.

II. SCOPE:

Departmentwide.

III. POLICY:

A. Some of the causes for disciplinary action are as follows. The list is not considered to be all-inclusive. Decisions regarding the severity of a disciplinary action are based on the seriousness or nature of the misconduct and/or prior disciplinary actions administered to the employee.

1. Has willfully violated any of the rules, regulations, policies or procedures of the Department after having been made aware of such.
2. Has willfully violated any of the provisions of the State Merit System Law or of the rules of the Personnel Advisory Board.
3. Is incompetent, inadequate, careless or inefficient in the performance of duties of their position (specific instances to be charged) or has failed to meet established minimum standards in the performance of such duties.
4. Has been wantonly careless or negligent in the care of the property of the state.
5. Has been guilty of abusive or improper treatment toward an inmate or patient of any state institution or to a person in custody, provided the acts committed were not necessarily or lawfully committed in self-defense, to protect the lives of others or to prevent the escape of anyone lawfully in custody.



ADMINISTRATIVE MANUAL

<p>SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action</p>	<i>Chapter:</i> 10
	<i>Section:</i> 10.4
<p>REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070 RSMo 36.410 and 105.262</p>	<i>Page:</i> 2 of 6
	<i>Revised:</i> 2-17-04

6. Has some permanent or chronic physical or mental ailment or defect, which incapacitates them for the proper performance of the duties of this position, including unrehabilitated alcoholism or narcotics addiction.
7. Has been habitually tardy in reporting for duty or has absented themselves frequently from duty during the course of regular working hours or has been completely absent from duty without prior or subsequent authorization for such absences.
8. Has been convicted of a felony or of a misdemeanor involving moral turpitude.
9. Has been guilty of a scandalous and disgraceful conduct while on or off duty where such conduct tends to bring the state service into public disrepute, or has exhibited behavior which adversely affects the employee's job performance, the employing agency, or both.
10. Has been guilty of abusive or improper treatment of guests or clients while on duty at any state facility or on any state land normally open to the public.
11. Has submitted a false statement of a material fact or has practiced or attempted to practice any fraud or deception in an application or examination or in otherwise attempting to secure employment subject to the provisions of these rules.
12. Has been guilty of insubordination or has failed to respond in a reasonable manner to the lawful orders or instructions of persons with duly delegated authority over the employee.
13. Has been abusive or physically violent toward other employees while on duty or in the duty area or has willfully exhibited behavior which is disruptive of the working activities of other employees.
14. Has been intoxicated or under the influence of a controlled substance while on duty except as may have been required by a licensed medical physician.
15. Has practiced or attempted to practice fraud or deception in securing or attempting to secure benefits or grants from a state agency either for himself or for another applicant.
16. Refuses to cooperate fully and truthfully with any formal or informal investigation, hearing or panel conducted by anyone within the Department or other state agency or body authorized to conduct same.



ADMINISTRATIVE MANUAL

SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action	<i>Chapter:</i> 10
	<i>Section:</i> 10.4
REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070 RSMo 36.410 and 105.262	<i>Page:</i> 3 of 6
	<i>Revised:</i> 2-17-04

17. Has failed to pay state income taxes or has failed to otherwise comply with the provisions of RSMo 105.262, and DHSS Policy 15.6, Employee Obligation to Pay State Income Taxes.
- B. Any situation in which disciplinary action is being recommended or initiated should be discussed with the Office of Personnel (OP). The Incident Report form may be used to gather all relevant information for misconduct situations in which a supervisor may potentially recommend disciplinary action for an employee (see Attachment A). The supervisor should make reference to the disciplinary action in the next performance appraisal. A special performance appraisal may be initiated depending on the nature of the situation.
 - C. It is the responsibility of supervisors and managers to administer discipline in a consistent, impartial and constructive manner and to prepare and maintain documentation to support disciplinary actions. Discipline may be imposed by an employee’s immediate supervisor or other management staff in the chain of command.

IV. GUIDELINES FOR DISCIPLINARY ACTION

There may be situations which require the supervisor to deal with an employees’ performance or behavior by recommending a disciplinary action. Such actions should be taken in consultation with the chain of command and the OP. Documentation is a key factor to be considered in any disciplinary action. Documentation needs to be clear, timely and behaviorally specific. Documentation for any of the types of disciplinary actions in Section V should include the following:

1. Was the employee aware of the rule, policy, procedure or expectation at the time of the violation?
2. Has the violation or incident been thoroughly investigated to determine the facts? Do you have written statements from witnesses? (The Incident Report form will assist you with this.)
3. What did or did not happen? Use words to paint a very clear picture. Explain in simple, objective, precise language exactly what happened. Specific dates, times,



ADMINISTRATIVE MANUAL

<p>SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action</p>	<p><i>Chapter:</i> 10</p>
	<p><i>Section:</i> 10.4</p>
<p>REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070 RSMo 36.410 and 105.262</p>	<p><i>Page:</i> 4 of 6</p>
	<p><i>Revised:</i> 2-17-04</p>

places and circumstances of the event should also be recorded. The Incident Report is a useful tool to use in gathering information.

4. What is the employee’s perspective with regard to the occurrence? Get the employee’s side of the story in writing.
5. Why is this event being documented? Explain how the event relates to and affects the employee’s performance, the performance of others, and the goals, objectives, or mission of the agency. What is its impact?
6. Is the disciplinary action being applied consistently? What has been the consequence for other employees committing a similar infraction?
7. What are the consequences? Explain what may happen if the necessary improvement is not made by the specified time or if the act occurs again (i.e., further disciplinary action up to and including dismissal).

V. TYPES OF DISCIPLINARY ACTIONS

- A. The following are disciplinary measures to be considered. Depending upon the severity of offenses, discipline may be implemented at any step determined to be appropriate, without requirement to use it progressively or incrementally. In some instances, immediate dismissal may be warranted.

Written Reprimand: Address the items in Section IV. Reprimands are generally issued under the supervisor’s/manager’s signature. The subject line of the memo will be, “Written Reprimand.” The last line of the memo will state that a copy will be placed in the employee’s official file in the OP. Note: See V.B. for instructions on presentation to employee.

Unacceptable Conduct: Address the items in Section IV. This is a letter issued under the Appointing Authority’s signature. A request for a Notice of Unacceptable Conduct is to be submitted through administrative channels to OP. The OP prepares the letter for the Appointing Authority’s signature. The letter will be presented to the employee by the supervisor or manager in a conference. This form of disciplinary action is also entered into the employee’s record at the Office of Administration/Division of Personnel. Note: See V.B. for instructions on presentation to employee.



ADMINISTRATIVE MANUAL

SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action	<i>Chapter:</i> 10
	<i>Section:</i> 10.4
REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070 RSMo 36.410 and 105.262	<i>Page:</i> 5 of 6
	<i>Revised:</i> 2-17-04

Suspension: Suspension is time away from work without pay. This action is taken by the Appointing Authority. A request for suspension, addressing the items in Section IV, is to be submitted through administrative channels to OP. The OP prepares the notification to the employee for the signature of the Appointing Authority. Note: See V.B. for instructions on presentation to employee.

Involuntary Demotion: This type of disciplinary action may be considered if the employee has previously held regular status in the position they are being demoted to, or are eligible for such position. This action requires the approval of the Appointing Authority, and a request for such action explaining why this is the most viable option shall be submitted through administrative channels to OP. The OP will prepare the notification to the employee for signature of the Appointing Authority. Note: See V.B. for instructions on presentation to employee.

Dismissal: This action is issued only by the Appointing Authority. A request for dismissal, addressing the items in Section IV, is to be submitted through administrative channels to OP. The OP prepares the notification to the employee for signature of the Appointing Authority. In most instances, the original document is given to the employee in a conference. Note: See V.B. for instructions on presentation to employee.

Dismissal Without Prejudice: If the Appointing Authority determines the circumstances warranting dismissal do not reflect discredit on the character or conduct of the employee, he/she may dismiss the employee “without prejudice.” This may apply to situations in which an employee was unable to meet expectations due to a medical condition, extensive absences brought on by a medical condition, etc. See V.B. for instructions on presentation to employee.

B. Presentation Instructions:

1. In most instances, the supervisor and/or manager/bureau chief gives the original document to the employee in a conference. The supervisor obtains the employee’s signature acknowledging receipt and forwards the receipt notice containing original signatures, along with a copy of the disciplinary action, to the OP for the employee’s official personnel records.



ADMINISTRATIVE MANUAL

<p>SUBJECT: PROBATION, PERFORMANCE APPRAISAL AND DISCIPLINE Disciplinary Action</p>	<p><i>Chapter:</i> 10</p>
	<p><i>Section:</i> 10.4</p>
<p>REFERENCES: State Personnel Division Rules Manual – 1 CSR 20-3.070 RSMo 36.410 and 105.262</p>	<p><i>Page:</i> 6 of 6</p>
	<p><i>Revised:</i> 2-17-04</p>

2. If the employee refuses to sign, the supervisor and one other person sign as witnesses that the employee received the document. The other witness must be a manager/supervisor or confidential secretary to the manager/supervisor. Never use a co-worker as a witness. In some cases, the employee may not be available for personal presentation, in which case the document is sent via certified mail. The return receipt is then sent to OP for inclusion in the employee’s official personnel file.

3. An employee shall be entitled to Union or non-Union co-worker representation to provide advice, assistance, or representation upon request if the employee is questioned by an agency representative about a matter that the employee reasonably believes may lead to a notice of unacceptable conduct, a notice of conditional employment, demotion, suspension or dismissal of the employee. Management shall allow approximately fifteen minutes conference time between Union or co-worker representative and employee prior to investigatory/disciplinary meetings. If management is certain that the situation will not result in disciplinary action of the aforementioned magnitude, management can so inform the employee and deny representation.

Prepared by:

Approved by:

Chief, Office of Personnel

Chief Operating Officer

Confidentiality Statement
Central Office
Missouri Department of Health and Senior Services
Bureau of HIV, STD, and Hepatitis

EMPLOYEE OATH OF CONFIDENTIALITY:

I hereby acknowledge that I will abide by the appropriate state statutes, regulations, protocols, and policies, regarding the confidentiality and security of HIV/AIDS, STD, and hepatitis surveillance data and information. I will not release HIV/AIDS, STD, or hepatitis surveillance data or information to any individual not granted authorization by the Missouri Department of Health and Senior Services (MDHSS) Bureau of HIV, STD, and Hepatitis. I will contact the Chief, Bureau HIV, STD, and Hepatitis, 573/751-6439 for any questions regarding the release of confidential information and to report breaches or suspected breaches of confidentiality. [Appropriate release of information is defined in the *Bureau of HIV, STD, and Hepatitis Confidentiality and Security Manual*. This manual defines statewide policy and protocols for the security of HIV/AIDS surveillance information.]

Penalties for unauthorized disclosure of confidential data or information are outlined in Missouri statute, RSMo 191.656. In addition to penalties under RSMo 191.656, violation of these standards is subject to disciplinary actions that could include suspension, demotion, or termination (MDHSS Administrative Manual, Chapter 10, Section 10.4).

I have received copies of the *Bureau of HIV, STD, and Hepatitis Confidentiality and Security Manual*, state statute RSMo 191.656, and the MDHSS administrative rule. I understand the consequences of violating confidentiality of any HIV/AIDS, STD, or hepatitis data or information.

Employee Signature and Date

Witness Signature and Date

CONFIDENTIALITY STATEMENT
Missouri Department of Health and Senior Services
Bureau of HIV, STD, and Hepatitis

ST. LOUIS CITY DEPARTMENT OF HEALTH AND HOSPITALS
HIV/AIDS, STD, AND HEPATITIS SURVEILLANCE PROGRAM

EMPLOYEE OATH OF CONFIDENTIALITY:

I hereby acknowledge that I will abide by the appropriate state statutes, regulations, protocols, and policies regarding the confidentiality and security of HIV/AIDS, STD, and hepatitis surveillance data and information. I will not release HIV/AIDS, STD, or hepatitis surveillance data or information to any individual not granted authorization by the Missouri Department of Health and Senior Services (MDHSS), Bureau of HIV, STD, and Hepatitis. I will report local breaches or suspected breaches of confidentiality to the local Overall Responsible Party [ORP] (when designated). The point of contact for any questions regarding release of information is the Disease Surveillance Unit Manager, Bureau of HIV, STD, and Hepatitis, 573/751-6119. [Appropriate release of information is defined in the *Bureau of HIV, STD, and Hepatitis Confidentiality and Security Manual*. This manual defines statewide policy and protocols for the security of HIV/AIDS, STD, and hepatitis surveillance information.]

Penalties for unauthorized disclosure of confidential data or information are outlined in Missouri statute, RSMo 191.656. In addition to penalties under RSMo 191.656, violation of these standards is subject to disciplinary actions that could include suspension, demotion, or termination.

I have received copies of the *Bureau of HIV, STD, and Hepatitis Surveillance Confidentiality Manual*, state statute RSMo 191.656, and the MDHSS administrative rule. I understand the consequences of violating confidentiality of any HIV/AIDS, STD, or hepatitis data or information.

Employee Signature and Date

Reviewer Signature and Date

CONFIDENTIALITY STATEMENT
Missouri Department of Health and Senior Services
Bureau of HIV, STD, and Hepatitis

KANSAS CITY HEALTH DEPARTMENT
HIV/AIDS, STD, AND HEPATITIS SURVEILLANCE PROGRAM

EMPLOYEE OATH OF CONFIDENTIALITY:

I hereby acknowledge that I will abide by the appropriate state statutes, regulations, protocols, and policies, regarding the confidentiality and security of HIV/AIDS, STD, and hepatitis surveillance data and information. I will not release HIV/AIDS, STD, and hepatitis surveillance data or information to any individual not granted authorization by the Missouri Department of Health and Senior Services (MDHSS), Bureau of HIV, STD, and Hepatitis. I will report local breaches or suspected breaches of confidentiality to the local Overall Responsible Party [ORP] (when designated). The point of contact for any questions regarding release of information is the Disease Surveillance Manager, Bureau of HIV, STD, and Hepatitis, 573/751.6119. [Appropriate release of information is defined in the *Bureau of HIV, STD, and Hepatitis Confidentiality and Security Manual*. This manual defines statewide policy and protocols for the security of HIV/AIDS, STD, and hepatitis surveillance information.]

Penalties for unauthorized disclosure of confidential information are outlined in Missouri statute, RSMo 191.656. In addition to penalties under RSMo 191.656, violation of these standards is subject to disciplinary actions that could include suspension, demotion, or termination.

I have received copies of the *Bureau of HIV, STD, and Hepatitis Surveillance Confidentiality Manual*, state statute RSMo 191.656, and the MDHSS administrative rule. I understand the consequences of violating confidentiality of any HIV/AIDS, STD, or hepatitis data or information.

Employee Signature and Date

Reviewer Signature and Date

12/01/05

**Confidentiality Statement
Tuberculosis Program**

**Missouri Department of Health and Senior Services
Bureau of HIV, STD, and Hepatitis**

EMPLOYEE OATH OF CONFIDENTIALITY:

I hereby acknowledge that I will abide by the appropriate state statutes, regulations, protocols, and policies, regarding the confidentiality and security of HIV/AIDS, STD, and hepatitis surveillance data and information. I will not release HIV/AIDS, STD, or hepatitis surveillance data or information to any individual not granted authorization by the Missouri Department of Health and Senior Services (MDHSS), Bureau of HIV, STD, and Hepatitis. I will refer any questions regarding release of information to the Chief, Bureau of HIV, STD, and Hepatitis, 573/751-6439. [Appropriate release of information is defined in the *Bureau of HIV, STD, and Hepatitis Confidentiality and Security Manual*. This manual defines statewide policy and protocols for the security of HIV/AIDS, STD, and hepatitis surveillance information.]

Penalties for unauthorized disclosure of confidential data or information are outlined in Missouri statute, RSMo 191.656. In addition to penalties under RSMo 191.656, violation of these standards is subject to disciplinary actions that could include suspension, demotion, or termination (MDHSS Administrative Manual, Chapter 10, Section 10.4).

I have received copies of RSMo 191.656 and the MDHSS administrative rule. I understand the consequences of violating confidentiality of any HIV/AIDS, STD, or hepatitis data or information.

Employee Signature and Date

Witness Signature and Date

Confidentiality Statement
Information Technology Services Division (ITSD)
Missouri Department of Health and Senior Services
Bureau of HIV, STD, and Hepatitis

EMPLOYEE OATH OF CONFIDENTIALITY:

I hereby acknowledge that I will abide by the appropriate state statutes, regulations, protocols, and policies, regarding the confidentiality and security of HIV/AIDS, STD, and hepatitis surveillance data and information. I will not release HIV/AIDS, STD, or hepatitis surveillance data or information to any individual not granted authorization by the Missouri Department of Health and Senior Services (MDHSS), Bureau of HIV, STD, and Hepatitis. I will refer any questions regarding release of information to the Chief, Bureau of HIV, STD, and Hepatitis, 573/751-6439. [Appropriate release of information is defined in the *Bureau of HIV, STD, and Hepatitis Confidentiality and Security Manual*. This manual defines statewide policy and protocols for the security of HIV/AIDS, STD, and hepatitis surveillance information.]

Penalties for unauthorized disclosure of confidential data or information are outlined in Missouri statute, RSMo 191.656. In addition to penalties under RSMo 191.656, violation of these standards is subject to disciplinary actions that could include suspension, demotion, or termination (MDHSS Administrative Manual, Chapter 10, Section 10.4).

I have received copies of RSMo 191.656 and the MDHSS administrative rule. I understand the consequences of violating confidentiality of any HIV/AIDS, STD, or hepatitis data or information.

Employee Signature and Date

Witness Signature and Date

**CERTIFICATION REGARDING COMPLIANCE WITH SECURITY STANDARDS FOR
THE PROTECTION OF HIV/AIDS, STD, AND HEPATITIS SURVEILLANCE
INFORMATION AND DATA
MISSOURI DEPARTMENT OF HEALTH AND SENIOR SERVICES**

The undersigned has been designated as the overall responsible party (ORP) by the applicant organization. This official accepts overall responsibility for implementing and enforcing the security standards and may be liable for breach of confidentiality. The ORP should be a high-ranking public health official, for example, the division director or bureau chief over HIV/AIDS, STD, and hepatitis surveillance. This official should have the authority to make decisions about surveillance operations that may affect programs outside HIV/AIDS, STD, and hepatitis surveillance unit and should serve as one of the contacts to public health professionals and the HIV affected community on policies and practices associated with HIV/AIDS, STD, and hepatitis surveillance.

By signing, the ORP certifies that the applicant will comply with the “*Security Standards for the Protection of HIV/AIDS Surveillance Information and Data*” by:

- (a) Applying the “**Program Requirements**” to all local/state/territorial staff and contractors funded through CDC to perform HIV/AIDS, STD, and hepatitis surveillance activities.
- (b) Applying the “**Program Requirements**” at all sites where the Enhanced HIV/AIDS Reporting System (eHARS) is maintained.

Name and address of organization Missouri Department of Health and Senior Services Section for Disease Control and Environmental Epidemiology 930 Wildwood Drive PO Box 570 Jefferson City, Missouri 65102	
Phone no. (with area code)	Fax no. (with area code)
Name of ORP (print)	Title
Signature	Date

**CERTIFICATION REGARDING COMPLIANCE WITH SECURITY STANDARDS FOR
THE PROTECTION OF HIV/AIDS, STD, AND HEPATITIS SURVEILLANCE
INFORMATION AND DATA
MISSOURI DEPARTMENT OF HEALTH AND SENIOR SERVICES**

The undersigned has been designated as the overall responsible party (ORP) by the applicant organization. This official accepts overall responsibility for implementing and enforcing the security standards and may be liable for breach of confidentiality. The ORP should be a high-ranking public health official, for example, the division director or department chief over HIV/AIDS, STD, and hepatitis surveillance. This official should have the authority to make decisions about surveillance operations that may affect programs outside HIV/AIDS, STD, and hepatitis surveillance unit and should serve as one of the contacts to public health professionals and the HIV affected community on policies and practices associated with HIV/AIDS, STD, and hepatitis surveillance.

By signing, the ORP certifies that the applicant will comply with the “*Security Standards for the Protection of HIV/AIDS Surveillance Information and Data*” by:

- (a) Report all breaches or suspected breaches of confidentiality occurring within the Surveillance jurisdiction (as defined in Scope of Work) to statewide ORP or designate (Chief, Bureau of HIV, STD, and Hepatitis).
- (b) Adherence to all statewide policy and procedures as outlined in the *Bureau of HIV, STD, and Hepatitis Confidentiality and Security Manual*.

St. Louis City Department of Health and Hospitals 634 North Grand, Suite 436 St. Louis, Missouri 63103	
Phone no. (with area code)	Fax no. (with area code)
Name of ORP (print)	Title
Signature	Date

**CERTIFICATION REGARDING COMPLIANCE WITH SECURITY STANDARDS FOR
THE PROTECTION OF HIV/AIDS, STD, AND HEPATITIS SURVEILLANCE
INFORMATION AND DATA
MISSOURI DEPARTMENT OF HEALTH AND SENIOR SERVICES**

The undersigned has been designated as the overall responsible party (ORP) by the applicant organization. This official accepts overall responsibility for implementing and enforcing the security standards and may be liable for breach of confidentiality. The ORP should be a high-ranking public health official, for example, the division director or department chief over HIV/AIDS, STD, and hepatitis surveillance. This official should have the authority to make decisions about surveillance operations that may affect programs outside HIV/AIDS, STD, and hepatitis surveillance unit and should serve as one of the contacts to public health professionals and the HIV affected community on policies and practices associated with HIV/AIDS, STD, and hepatitis surveillance.

By signing, the ORP certifies that the applicant will comply with the “*Security Standards for the Protection of HIV/AIDS Surveillance Information and Data*” by:

- (a) Report all breaches or suspected breaches of confidentiality occurring within the Surveillance jurisdiction (as defined in Scope of Work) to statewide ORP or designate (Chief, Bureau of HIV, STD, and Hepatitis).
- (b) Adherence to all statewide policy and procedures as outlined in the *Bureau of HIV, STD, and Hepatitis Confidentiality and Security Manual*.

Kansas City Health Department 2400 Troost Ave. Kansas City, MO 64108	
Phone no. (with area code)	Fax no. (with area code)
Name of ORP (print)	Title
Signature	Date

Individual Office Security Checklist - HIV/AIDS, STD, and Hepatitis Surveillance

A. Hard Copy Data

1. All HIV/AIDS, STD, and hepatitis data containing patient identifiers are stored in (double) locked storage (e.g., file cabinets with bar locks) when not under current investigation or at the end of each day.
2. Keys to locked file cabinets are securely maintained.
3. Confidential documents are placed out of view or secured when absent from workstations for short periods of time or at the end of each day.
4. Documents containing personal identifiers (e.g., case reports, phone messages) are shredded when no longer needed.

B. PC Data/Workstations

1. Passwords are kept confidential and not recorded in the workstation.
2. Documents containing personal identifiers are stored in appropriate database (i.e., eHARS, or other supplemental database) or on confidential drives.
3. Confidential information is not left on-screen when absent from workstation.
4. Screen saver is set for lowest time interval (preferably 1-2 minutes).
5. Staff should log out of network when absent from workstations for extended periods of time (defined as 2 hours) and at the end of each day.
6. All disks containing confidential information are forwarded to the data manager or other authorized personnel for proper erasure (Norton's WipeInfo) when no longer needed.
7. All surplus computers are sent to the data manager for processing and then forwarded to ITSD staff to ensure appropriate erasure.

C. Transfer/Release of Data

1. Line listings containing patient information are never released.
2. Names and personal identifiers are used in written correspondence only when necessary; and status not identified, wherever possible.
3. Addressee is informed that confidential correspondence is being faxed, and all correspondence is addressed/sent directly to the correct person. Addressee should be instructed to contact sender if correspondence is not received within the expected timeframe. For facsimile transmission, a dedicated line is used.
4. Staff should assure that confidential information communicated by phone is released only to appropriate authorized personnel and precautions taken to insure that personnel are authorized (e.g., call back verification).
5. Information with personal identifiers should not be left on answering machine or voice mail unless determined to be a secured line.

6. Incoming phone calls are answered generically (e.g., “Department of Health and Senior Services”, “This is _____”).
7. Staff should discuss confidential information only in secure, private areas and be conscious of the environment (e.g., visitors).
8. Small cell information is not released without the authorization of the HIV/AIDS Surveillance Coordinator, HIV/AIDS Surveillance Program.
9. Patient information is not released without the authorization of the HIV/AIDS Surveillance Coordinator, HIV/AIDS Surveillance Program.
10. Confidential information is not left in common work areas (i.e., photocopier, printer, fax).

D. Out-of-Office Security Measures

1. All line listings or written information containing personal identifiers are removed from office only when necessary (i.e., medical record reviews, validation studies), and do not contain direct references to HIV/AIDS, STD, and hepatitis.
2. Confidential information is never left unattended.
3. Field activities are conducted in secure and confidential areas as possible.
4. Laptops and other portable devices that receive or store HIV/AIDS, STD, and hepatitis surveillance information must use encryption software that meets the 128-bit encryption standard. Before taking any device containing sensitive information out of the secured area, the data must be encrypted.

Attachment 14

**MISSOURI DEPARTMENT OF HEALTH AND SENIOR SERVICES (DHSS)
STATEMENT OF AGREEMENT TO MAINTAIN CONFIDENTIALITY OF RECORDS AND
INFORMATION IN ACCORDANCE WITH DHSS POLICIES**

Code of Conduct

Interns, contractors or volunteers working under supervision of DHSS employees, whether paid or unpaid, shall be considered as employees with respect to the DHSS confidentiality policies. All information that identifies or can be used to readily identify individuals shall be considered confidential. All employees shall follow the DHSS policies for sharing of confidential information. Information specifically covered by the federal Standard for Privacy of Individually Identifiable Health Information (45 CFR 160 and 164) shall be determined and employees with responsibilities requiring access to the information identified. These employees shall attend expanded training and comply with DHSS policies relating to the federal laws.

Employees

As a DHSS employee, I agree to be knowledgeable of and comply with DHSS confidentiality policies.

Specifically I agree to:

- ✓ Assure the confidentiality and security of all information by limiting access to those having an official need in order to perform their duties;
- ✓ Restrict disclosure of confidential information to other agencies or individuals outside of DHSS. Disclosures shall be made in accordance with DHSS policies governing disclosures;
- ✓ Refrain from disclosing confidential personnel information to any individual or entity who does not have a business-related reason to receive such information.
- ✓ Participate in training, as needed, on the federal Privacy law;
- ✓ Make appropriate staff aware of potential DHSS confidentiality policy violations; and
- ✓ Sign an annual statement affirming agreement to comply with DHSS confidentiality policies.

Contractors

As a DHSS contractor, I agree to maintain strict confidentiality of all information that identifies or can be readily used to identify individuals that I have been provided access to by the DHSS or obtained as a result of contract activities. I understand there are potential legal penalties for breaches of confidentiality or unauthorized destruction of confidential information/records. I understand that the contracting agency assumes liability for all disclosures of confidential information by the contractor and/or the contractor's employee.

Researchers

As a researcher being granted access to DHSS information and data for research purposes, I agree to comply with DHSS confidentiality policies. I agree to maintain the confidentiality of information that identifies individuals. I also agree not to subsequently disclose confidential information without written permission of the Department and/or individual person. For research projects requiring access to information covered under the federal Standard for Privacy of Individually Identifiable Health Information (45 CFR 160 and 164), I agree to comply with the federal requirements.

Volunteers

As a volunteer, paid or unpaid, I agree to comply with the DHSS confidentiality policies. I understand that I am liable for all breaches of confidentiality and may be subject to possible legal actions.

MAINTAINING CONFIDENTIALITY OF INFORMATION IN THE WORK ENVIRONMENT:

I agree to the following:

Work Areas

To remove information of a confidential nature from public view (placed inside a desk or file) when away from my work station and another authorized employee is not available to assure security of the information.

To place information of a confidential nature in locked files or other secure places when my office or work unit is closed or left unattended.

To shred or otherwise destroy information to be discarded that identifies an individual, such as poor quality copies or purged file materials.

Information Exchange

To not release confidential personnel information as obtained in the performance of duties to individuals or entities who do not have a business-related reason to receive such information.

To destroy informal records of telephone conversations containing information of a confidential nature unless the records are placed in official files.

To hold conferences and informal conversations in a manner to avoid discussions, of a confidential nature, being overheard by others.

To seal all documents containing information of a confidential nature inside an envelope addressed to a specific office or individual and marked "CONFIDENTIAL" when using conventional mail to send to other individuals, programs or agencies having an official need for the information.

To use a cover page containing a confidentiality statement approved by the DHSS Privacy Officer for all documents of a confidential nature transmitted by FAX machine to agencies and individuals with an official need to know.

To alert the receiver that the information is being transmitted via FAX and request immediate retrieval.

To include the DHSS approved statement of confidentiality on all electronic mail messages.

To not send confidential individually identifiable health information using electronic mail unless technology such as encryption or other technology is employed.

Computers

To comply with policies and procedures relating to maintaining security and confidentiality of computer data.

To position my computer workstation screen to limit visualization by other employees or visitors.

To protect my sign on and passwords to prevent others from using them.

To logout of the network when away from my work area for an extended period; for short periods of inactivity, I will activate a password protected screen saver.

Penalties

I have been informed and understand that a breach of confidentiality or unauthorized destruction of confidential records shall result in disciplinary action up to and including dismissal depending on the severity of the offense and possibly legal action.

CERTIFICATION:

This is to certify that I have read and agree to comply with the provisions of the Department's policies.

Date: _____ Signature: _____

Please print name: _____

NOTE: One copy should be signed and placed in employee's personnel file and the employee should retain one copy.