



Arkansas Department of Health

4815 West Markham Street Slot-33 • Little Rock, Arkansas 72205-3867 • Telephone (501) 661-2408

Governor Mike Beebe

Paul K. Halverson, DrPH, FACHE, Director and State Health Officer

Arkansas HIV/AIDS Surveillance

**Procedures,
Confidentiality/Security Policy
&
Confidentiality Pledge**

TABLE OF CONTENTS

STATEMENT OF CONFIDENTIALITY.....	2
INTRODUCTION.....	3
PURPOSE.....	3
REQUIREMENTS & STANDARDS.....	3
GUIDING PRINCIPLES.....	4
REQUIREMENTS.....	5
Policies.....	5
Responsibilities.....	7
Training.....	9
Physical Security.....	9
Data Security.....	11
Security Breaches.....	14
Laptops & Portable Devices.....	15
Removable & External Storage Devices.....	15



Arkansas Department of Health

4815 West Markham Street Slot-33 • Little Rock, Arkansas 72205-3867 • Telephone (501) 661-2408

Governor Mike Beebe

Paul K. Halverson, DrPH, FACHE, Director and State Health Officer

PURPOSE

This confidentiality and security manual has been established to ensure confidentiality of Human Immunodeficiency Virus (HIV) surveillance data. Arkansas state law ACT 614 of 1989 and ACT 967 of 1991 requires HIV/AIDS cases to be reported to the Department of Health (DOH) by physicians, hospitals, infection control practitioners and/or chairpersons of hospital infection control committees, directors of all laboratories doing business in the state of Arkansas, medical directors of in-home health agencies, program directors of all state agencies to whom an HIV/AIDS diagnosis has been disclosed, nursing home medical directors and other person as required by the rules and regulations of the Arkansas Department of Health (ADH).

POLICY

1. All mail address specifically to 'HIV/AIDS Surveillance Unit' is opened only by Surveillance staff.
2. Only Surveillance staff and authorized Information Technology staff have access to the Enhanced HIV/AIDS Reporting System (eHARS), the surveillance database used to track HIV/AIDS cases.
3. Every case reported to the Surveillance Unit is also reported to the Centers for Disease Control & Prevention. However, all personal identifiers are removed. Personal identifiers are only released to the physician or organization that reported the case.
4. Cases are entered in a computer system that is isolated from the network system. The computer is located in a inner office which is kept locked after normal working hours or when surveillance staffs are not available. Only surveillance staffs have a key.
5. Authorized surveillance staffs from other states are notified if a patient was diagnosed in their state and moved to Arkansas.
6. Persons infected with Tuberculosis (TB), as well as HIV, are referred to the TB Program to facilitate appropriate treatment for that individual.
7. Names and/or patient information will be released only to authorized persons stated above.
8. The Surveillance Unit adheres to a data release policy that ensures any HIV/AIDS data released and/or published are done so while maintaining confidentiality.

We respect and appreciate patient and physician concerns regarding confidentiality and security of HIV/AIDS data. Confidentiality is a top priority for the Surveillance unit. If you have any further questions, please call us at (501) 661-2971.

INTRODUCTION

The HIV/AIDS Surveillance Program, at the Arkansas Department of Health, is responsible for monitoring the HIV/AIDS epidemic in Arkansas in order to provide information to guide policy decisions, target resources, and help to evaluate services and prevention activities. This involves the collection, maintenance, and analysis of name-based HIV/AIDS information. All state HIV/AIDS surveillance systems are also responsible for maintaining the standards set by the Centers for Disease Control and Prevention (CDC), as outlined in the 2006 Technical Guidance for HIV/AIDS Surveillance Programs, Volume III.

HIV/AIDS case reporting by name and address (and other information) is required by the ACT 967 of 1991 and under the authority of the Rules and Regulations of the Arkansas State Board of Health pertaining to Communicable Disease Control. Regulatory CD4+ lymphocyte reporting for all CD4+ test results was approved by the Board of Health on July 29, 1994 and added to the list of Common Reportable Diseases, Condition and Findings.

Documents which could (directly or indirectly) identify a person with HIV or AIDS, as well as information obtained through a case investigation, case report, personal interview, database, or research study which may be suggestive of HIV or AIDS, are “confidential information” and are subject to specific regulations for maintenance of confidentiality. The personnel policies of the Arkansas Department of Health allow for the immediate termination of any found to have breached patient confidentiality.

The success of HIV/AIDS surveillance in Arkansas depends upon the trust and cooperation of the public and their health care providers. The State of Arkansas has statutes to protect individuals against HIV/AIDS discrimination. However, public attitudes cannot necessarily be changed; there could be devastating consequences if sensitive information about high risk behaviors or HIV status reached employers, insurers, schools, family or acquaintances. This may influence how persons at risk for HIV/AIDS choose to access testing and treatment. Because of these concerns, the Program and CDC constantly work to develop and maintain comprehensive, detailed security and confidentiality guidelines.

PURPOSE

The purpose of this document is to outline policies and procedures for handling confidential information maintained by Program. Confidential material refers to documents or data that clearly contain identifying information, primarily names. Other data collected, which do not contain patient-specific identifying information, may also be considered confidential. The

Program strives to provide aggregate data for maximum public health utility with minimum risk of disclosure of individual-level data.

REQUIREMENTS AND STANDARDS

CDC's 2006 Technical Guidance outlines guiding principles and requirements to guide surveillance staff and provide a basis for corrective action when conduct falls below the required minimum standards. This includes defining the standard of conduct that the public should expect of surveillance staff in protecting private and sensitive information. Each of the thirty-five (35) requirements outlined by CDC is addressed in this document by security-related topic. The five (5) guiding principles are the basis upon which all the requirements are derived.

GUIDING PRINCIPLES

Guiding Principle 1. HIV/AIDS surveillance information and data will be maintained in a physically secure environment.

- Refer to sections on Physical Security and Removable and External Storage Devices.

Guiding Principle 2. Electronic HIV/AIDS surveillance data will be held in a technically secure environment, with the number of data repositories and individuals permitted access kept to a minimum. Operational security procedures will be implemented and documented to minimize the number of staff that have access to personal identifiers and to minimize the number of locations where personal identifiers are stored.

- Refer to sections on Policies, Training, Data Security, Access Control, Laptops and Portable Devices, and Removable and External Storage Devices.

Guiding Principle 3. Individual surveillance staff members and persons authorized to access case-specific information will be responsible for protecting confidential HIV/AIDS surveillance information and data.

- Refer to sections on Responsibilities, Training, and Removable and External Storage Devices.

Guiding Principle 4. Security breaches of HIV/AIDS surveillance information or data will be investigated thoroughly, and sanctions imposed as appropriate.

- Refer to section on Security Breaches.

Guiding Principle 5. Security practices and written policies will be continuously reviewed, assessed, and as necessary, changed to improve the protection of confidential HIV/AIDS surveillance information and data.

- Refer to sections on Policies and Security and Confidentiality Program Requirement Checklist.

REQUIREMENTS

Policies

Requirement 1. Policies must be in writing

- This document, the Arkansas HIV/AIDS Security & Confidentiality Policy, will serve as the overall policy for all HIV/AIDS surveillance activities. It will be reviewed and revised, as deemed necessary, on an annual basis.

Requirement 2. A policy must name the individual who is the Overall Responsible Party (ORP) for the security system.

- The Overall Responsible Party (ORP) for the CDC cooperative Agreement for HIV/AIDS surveillance is Charles McGrew. Mr. McGrew serves as the Deputy Director and Chief operating Officer of the Arkansas Department of Health, charles.mcgreg@arkansas.gov, (501) 280-4061
- Current staff working directly on HIV/AIDS surveillance in the Program include:
 - Sharon Donovan, Section Chief
Sharon.donovan@arkansas.gov, (501) 661-2971
 - Keeven Murphy, Health Program Specialist I
keeven.murphy@arkansas.gov, (501) 661-2887
 - Cynthia Neal, Health Program Specialist I
cynthia.neal2@arkansas.gov, (501) 661-2599
 - Marie Wilson, Administrative Analyst
marie.wilson@arkansas.gov, (501) 280-4036

Requirement 3. A policy must describe methods for the review of security practices for HIV/AIDS surveillance data. Included in the policy should be a requirement for an ongoing review of evolving technology to ensure that data remain secure.

- Annual written reviews of security and confidentiality policies and procedures shall be conducted in conjunction with the employees' yearly performance evaluation.
- The addition of new technologies to surveillance activities (i.e., network use, software changes, etc.) shall be preceded by an evaluation of existing measures and/or the development of new measures to ensure the continued security of surveillance information and data.

- Surveillance staff receive annual training regarding confidential & security issues as addressed herein, and are required to read and retain a copy of this document and also sign a confidentiality pledge.

Requirement 4. Access to and uses of surveillance information or data must be defined in a data release policy.

- The Surveillance Unit shall release surveillance information for statistical purposes in such a manner that no identifiable information is released.
- To the extent necessary to comply with a proper judicial order requiring release of human immunodeficiency virus test results and related information to a prosecutor for an investigation of violation of ACT 438 of 1993.

Requirement 5. A policy must incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying.

- The Arkansas HIV/AIDS Release Policy includes contingencies for releasing data with both small numerators and denominators.

Requirement 6. Policies must be readily accessible by any staff having access to confidential surveillance information or data at the central level and, if applicable, at noncentral sites.

- A hardcopy of this policy resides in the Arkansas HIV/AIDS Surveillance Section and the HIV/STD Program Section and all staff have received a copy.

Requirement 7. A policy must define the roles for all persons who are authorized to access what specific information and, for those staff outside the surveillance unit, what standard procedures or methods will be used when access is determined to be necessary.

- Surveillance staffs only, are authorized to access all data that are received during daily surveillance activities. This includes hardcopies of reports and databases containing identifying information. Surveillance staffs require access to all these data in order to conduct follow-up on HIV cases.

Requirement 8. All authorized staff must annually sign a confidentiality statement. Newly hired staff must sign a confidentiality statement before access to surveillance data is authorized. The new employee or newly authorized staff must show the signed confidentiality statement to the grantor of passwords and keys before passwords and keys are assigned. This statement must indicate that the employee understands and agrees that surveillance information or data will not be released to any individual not granted access by the ORP. The original statement must be held in the employee's personnel file and a copy given to the employee.

- Each Program staff member working with confidential information must take the introductory and operational level courses for Health Insurance Portability and Accountability Act certification (HIPAA).

- Security and confidentiality training shall be provided to all new staff prior to handling of sensitive information. Staff granted access will have signed an Employee Statement of Confidentiality prior to being granted access. Compliance with these policies will be reviewed on a yearly basis and a new oath signed annually.
- Upon resignation or termination of employment, staff must sign another Statement of Confidentiality upon Separation the Section Chief must also ensure that all materials and keys have been returned and documented appropriately on the Separation Checklist.
- Access to work areas, computers, and confidential data will be restricted to Monday through Friday work days and during approved work hours. The Section Chief maintains a list of staff with access to data on the Staff Access Form.
- Staff take the annual HIPAA training
- Staff signs a yearly employee statement of confidentiality

Requirement 9. A policy must outline procedures for handling incoming mail to and outgoing mail from the surveillance unit. The amount and sensitivity of information contained in any one piece of mail must be kept to a minimum.

- Although the HIV/STD clerical staff receive and date stamp incoming mail, only Surveillance staff shall open confidential surveillance mail.
- All mailing labels and contact information will reflect an 'Attention to' line that specifies the name of the HIV/AIDS Surveillance Coordinator.
- All outgoing mail containing confidential information is double enveloped. The inner envelope is sealed, addressed and stamped "confidential". The outer envelope is addressed to the provider.
- Surveillance staff will work to ensure that all confidential surveillance mail shall not be identified with the words 'HIV' or 'AIDS' in any manner.
- Mail containing confidential information will be clearly marked "Confidential." Such mail will also be clearly marked with an explicit return address.

Responsibilities

Requirement 10. In compliance with CDC's cooperative agreement requirement, the ORP must certify annually that all program requirements are met.

- The ORP shall annually certify, as part of the CDC Cooperative Agreement, that Program requirements are met and security standards are in place. The ORP will be responsible for recertification

Requirement 11. Each member of the surveillance staff and all persons described in this document who are authorized to access case-specific information must be knowledgeable about the organization's information security policies and procedures.

- **Phone**
 - Staff must discuss patient information only with authorized persons in a manner that ensures the conversation cannot be overheard.
 - If the call is to or from an out-of-state surveillance system, the identity of the caller will be verified by referring to a list (maintained by the Council of State and Territorial Epidemiologists) of authorized surveillance staff prior to release of information. If not on the list, the supervisor of the contact will be called for verification.
 - Only Surveillance staff should take incoming calls with confidential information. If authorized staffs are not available, a message can be taken, but no confidential information should be taken.
 - Outgoing calls by Surveillance staff must be made with the utmost discretion when confidential information is being discussed. It is critical to ensure that the receiver of the information is legitimately authorized to receive confidential information.
 - People reporting confidential information shall not leave such information on the voicemail of Surveillance staff. Case information reported to other states will not be left on voicemail of other states.
 - When receiving a case report by phone, Surveillance staff shall not confirm whether or not the case has previously been reported. The exception to this rule occurs when working with either 1) local Disease Intervention Specialist (DIS) members that work for ADH; or 2) other state surveillance personnel. Sharing of information to these entities is necessary to carry out public health activities, including follow up and referral to partner services.

- **Photocopying**
 - All confidential material must remain in the Surveillance Unit as much as possible. If materials need to be photocopied outside the Surveillance Unit, only Surveillance staff may be designated to copy the materials.

- **Faxes**
 - Though faxes of confidential materials are generally discouraged by CDC, the Program has a fax machine located within its secured area. As a general rule, fax machines are not used to send or receive information containing personal identifiers. When identification of the Program may present a potential confidentiality problem, Program staff should substitute a generic ADH fax cover sheet.

- **Use of Fax to Send or Receive Sensitive Data**

As a general rule, fax machines are not used to send or receive information containing personal identifiers. However, it is occasionally necessary to fax lists of names (not identified as HIV or AIDS cases) to sites so that providers can pull medical records for review. In such cases, staff ensures that the appropriate person at the site is standing by

to receive the fax. In instances where providers request to fax information to Surveillance staff, staff arranges to be present at the fax machine as the fax is being received.

This requirement is being followed by all surveillance staff members

Requirement 12. All staff that is authorized to access surveillance data must be responsible for challenging those who are not authorized to access surveillance data.

- Upon starting work with the Program, all staff are immediately oriented to its activities and policies. This includes an explicit review of this policy, and thereafter on a yearly basis. As described under Requirement 8, staffs sign an Employee Statement of Confidentiality that state their understanding and adherence to Surveillance policies.
- Staff shall immediately report all suspected breaches of confidentiality to the ORP, or the Surveillance Coordinator. All staff must obtain and read the policy and sign the statement of their understanding and adherence to the policy.

Requirement 13. All staff that is authorized to access surveillance data must be individually responsible for protecting their own workstation, laptop, or other devices associated with confidential surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Staff must take care not to infect surveillance software with computer viruses and not to damage hardware through exposure to extreme heat or cold.

- As previously stated, staff sign an Employee Statement of Confidentiality that states their understanding and adherence to Program policies.
- Paperwork and computer monitors should not be observed by unauthorized personnel.
- Workstations/laptop are password protected and passwords are changed every ninety days; surveillance offices are locked when staff members are away from their workstation. Passwords should be at least 8 characters in length, at least one capital letter and at least one number.
- **Maintenance and Security of Documents Containing Confidential Information**
All confidential hard copy HIV and AIDS case information and other documents are maintained permanently in locked file cabinets within secured area of the Surveillance Unit.
- **Maintaining Security and Confidentiality During Field Activities**
While conducting routine surveillance work in the field, such as record reviews or hospital validation studies, Surveillance staff keeps confidential materials with them at all times. Confidential materials are never left in public access areas. Confidential material taken out of the Surveillance Unit is returned before the end of each workday, with the exception of field activities requiring overnight stay. During activities where overnight stay is required, patient information is listed by soundex codes and dates of birth. The patient names are attached to records once they are returned to the Surveillance Unit.
- **Internal Program Communications**

Surveillance staff, including full or part-time employees, may consult among themselves or share information with other staff within the program or with any person having direct administrative control over that program if the person has a “compelling need to know” the information (e.g. regarding medical management or completion of surveillance forms) in order to perform his or her job duties. Any staff member who requests confidential patient information without having a “need to know” in order to perform his or her job is denied access. These determinations will be made by the Surveillance Administrator or Surveillance Coordinator.

- **Communication with External Media Organizations**

All requests for information from outside media must be referred to Arkansas Department of Health Communication Coordinator, who will route the request to an authorized person within the Division of AIDS/STD or the Bureau of Public Health Programs.

- **Incoming Mail to the HIV/AIDS Surveillance Unit**

All incoming mail should be addressed specifically to “HIV/AIDS Surveillance”. The full mailing address is included on all case report forms. All incoming

HIV/AIDS

Surveillance mail is sorted by division clerical staff and delivered to and opened by HIV/AIDS Surveillance staff within the secured area.

- **Outgoing Mail from the HIV/AIDS Surveillance Unit**

All outgoing mail from the HIV/AIDS Surveillance Unit containing any confidential information is double enveloped. The inner envelope is sealed, addressed and stamped “confidential”. The outer envelope is addressed to provider. All outgoing mail is deposited in the Division mailbox in the secretarial area at the regular time of delivery to the Department’s mailroom.

Training

Requirement 14. Every individual with access to surveillance data must attend security training annually. The date of training must be documented in the employee's personnel file. Information Technology (IT) staff and contractors who require access to data must undergo the same training as surveillance staff and sign the same agreements. This requirement applies to any staff with access to servers, workstations, backup devices, etc.

- As stated above, these policies are reviewed on an annual basis at which time staff are required to sign another Employee Statement of Confidentiality. IT staff that support Surveillance functions are also included. The Section Chief is responsible for ensuring these trainings occur and documenting them appropriately in personnel files.
- During orientation, all new surveillance staffs are thoroughly trained on the methodology of HIV/AIDS surveillance including protocols for the HIV/AIDS Confidentiality/Security Policy. They are also trained on the directive to report all suspected breaches of confidentiality.

- Confidentiality updates/reviews are held annually. Updates allow for sharing of information regarding confidentiality/security including discussion of new policy, review of existing policy, and review of CDC program requirements.
- All non-surveillance staff including IT personnel authorized to access surveillance information is also provided confidentiality/security training on an annual basis.
- A member of the Surveillance will attend all CDC recommended or required confidentiality trainings.

Physical Security

Requirement 15. All physical locations containing electronic or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access. Workspace for individuals with access to surveillance information must also be within a secure locked area.

- Surveillance staffs offices are private and not shared with other non-HIV ADH staff and locked whenever staff are not in them. Case report forms, files, laboratory reports, diskettes, and any other materials that contain patient identifiers will be closed and placed in locked cabinets when not in use and after normal working hours.
- All hard copy documents are concealed or locked in a file cabinets or desk within the secured area when employees are absent from their individual workstations for even a brief periods of time.
- Other staffs or visitors must knock and receive permission to enter Surveillance offices. All documents and computers that contain surveillance information are to be secured before visitors enter the area.
- Only staffs that work directly for the Surveillance Unit have keys to the Surveillance offices. Keys are not held by staff outside the Program, building maintenance, or building security.
- The Section Chief maintains a list of all staff that has keys to the secured offices and cabinets on the Staff Access Form. All offices are locked when staff is away from unit; all forms, files and other materials are kept in locked cabinets that are secured in the surveillance unit.
- **Computer Output and Other Confidential Materials or Documents That Do Not Require Storage**
Visual access to forms and computer output shall be restricted to HIV/AIDS Surveillance staff unless authorized by the HIV/AIDS Surveillance Coordinator or the Administrator of HIV/AIDS Surveillance. All line lists, internal and external documents containing directly- or indirectly- identifying information are kept in locked file cabinets or desks within the secured area. All confidential documents such as telephone messages, old line lists and computer printouts which contain names are shredded when no longer needed. Backup diskettes are kept in locked file cabinets within Surveillance Unit.
- **Physical Access to Computers and Data**

All case information is entered into microcomputers, which are linked to a LAN network. This network is password protected and accessible by Surveillance staff only. Offices containing computers and diskettes are secured each night, and access to these offices is restricted to Surveillance personnel requiring access to patient identifiers as part of their job duties. All computers data, backup diskettes and other confidential information are locked in file cabinets within the Surveillance section.

Requirement 16. Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room.

- Access to the Surveillance Unit offices and equipment, including hard copy files containing identifying patient data, shall be restricted to Surveillance staff unless specifically authorized by the Section Chief.
- Visitors are not permitted in the Surveillance offices unless there is a surveillance staff present. All staff working in the vicinity of the Surveillance Unit is to question any strangers in the area and immediately report to the Section Chief any suspicious behavior.
- Only printers directly attached to Program computers are to be used for printing of confidential information. In the case that network printers must be used, Program staff must promptly pick up their printouts.
- All hard copies of surveillance information are securely stored and maintained in the Surveillance Unit in locked file cabinets.
- The Surveillance Coordinator retains the keys to hard copy storage. However, all staffs are responsible for insuring security of their individual workstations, including appropriate storage of hard copy files. Staffs are following each of the steps in this requirement.
- **Use of computer-Generated Line Lists Containing Personal Identifiers**
Minimal information necessary to perform follow-up or other surveillance activity is generated in the form of line lists which are locked in file cabinets in the secured area and shredded when the activity is completed.

Requirement 17. Each member of the surveillance staff must shred documents containing confidential information before disposing of them. Shredders should be of commercial quality with a crosscutting feature.

- After case reports have been entered into the Enhanced HIV/AIDS Reporting System (eHARS) and filed in the Program offices, duplicate copies are shredded.
- Other duplicated confidential data must be shredded or erased electronically when no longer needed. Documents are shredded with commercial quality shredders with a crosscutting or confetti feature prior to disposal. Electronic data undergoes a full wipe, per standards set by the U.S. Department of Defense. Surveillance documents that needs to shredded is being shredded by a surveillance staff member using commercial quality shredders

Requirement 18. Rooms containing surveillance data must not be easily accessible by window.

- The HIV/AIDS Surveillance unit is located on the fourth floor of the Arkansas Health Department. Therefore, the unit is not accessible by windows. The window that does exist in the current offices is shielded by vertical blinds and is above street level.
- Building access is restricted with only one entrance open for the public. Policemen are posted inside the Health Department while the building is open.
- A security station is located at the public entrance; all visitors are required to register and to display a visitor identification badge. Offices are not accessible by windows

Data Security

Requirement 19. Surveillance information must have personal identifiers removed (an analysis dataset) if taken out of the secured area or accessed from an unsecured area.

- It is the Surveillance Unit practice to strip identifiers out of datasets to be used for analysis; this includes those that are removed from a secured area or accessed in an unsecured area.
- Electronic data in eHARS otherwise resides on a secured server at the ADH Data Center. The server is in a locked rack in a locked, environmentally-controlled room with limited access by IT staff.
- The current deployment of eHARS does not allow for information to be accessed from a remote or unsecured area; remote or unsecured areas include workstations outside of offices dedicated to Program staff. To access eHARS, Program staff must use personal log-ins at their assigned computer workstation during regular work hours
- Due to current regulations in Section 1.18.665, Arkansas Administrative Code, the Program must keep all hardcopies of data on each case for a minimum of ten (10) years; these currently reside in locked cabinets in the Program's secured area. The Program is working with retention officials to address an earlier disposal schedule for reports that have been transferred to eHARS. At such time that paper copies must be archived and removed from the Program's secured area, the Program will take all steps to de-identify documents prior to off-site storage. Each step is being followed and no documents are being stored off-site.
- **Reporting of Case Data to the Centers for Disease Control**
All HIV/AIDS case data is transmitted by the Secure Data Network to the Centers for Disease Control and Prevention (CDC) by the last week of each month. However, all personal identifiers such as names and addresses are deleted. For reporting purposes, CDC uses a soundex code of a person's last name in order to prevent possible identification of any reported individual.
- **Release of Information to Out-of State Surveillance Programs**
When HIV/AIDS case information is obtained on any person who currently resides or

previously resided in any state outside Arkansas, authorized HIV/AIDS Surveillance personnel in those states (CDC provides lists of authorized names and contacts in each state) will be contacted by designated Arkansas HIV/AIDS Surveillance staff and provided said information. When out-of-state surveillance personnel contact the Arkansas HIV/AIDS Surveillance Unit, the information is collected, the caller's name and phone number are obtained and the caller is told that he or she will receive a call back with the information requested. No information is provided until the caller's name and phone number are verified with the CDC listing.

- **Release of Information to Reporting Sites**

Patient information or line lists of their respective cases may be provided back to the physicians or infection control practitioners of reporting sites. When confidential information is mailed, it is placed in double envelopes. The inner envelope is stamped "confidential", and will be addressed to a specific person or provider.

- **Release of Information to Physicians or Infection Control**

Practitioners Calling to Report HIV/AIDS Cases

Frequently, prior to completing a case report form, infection control practitioners or physicians may call the HIV/AIDS Surveillance Unit to report a case and may inquire if a patient has been previously reported. If the person calling to report a case or requesting information is not known to Surveillance staff and the request information is considered to be legitimate, the information taken and/or provided by telephone.

If Surveillance staff does not know the person requesting the information, the information is taken but no information will be released. After the call, authorized Surveillance staff will look up the phone number of the hospital ICP or physician who called to report the case and will call them back in order to verify that the person who reported the case is legitimate.

Release of Information to Disease Intervention Specialist for Partner Notification Purposes

Copies of case report forms for all new cases of HIV and AIDS are provided to the Division's Epidemiology staff within one working day after completion of the form. The Epidemiology staff enters case information into the STD-MIS and a field record is initiated to the Division's Disease Intervention Specialist (DIS) staff for counseling

and

partner notification purposes. The copy of the case report is attached to the Field Record when initiated to the field, and is later filed in the patient's record in the health unit. The DIS is not required to obtain consent from the patient's attending physician prior to contacting the patient. Surveillance staff review all completed STD records to obtain risk and other AIDS-defining information.

Requirement 20. An analysis dataset must be held securely by using protective software (i.e., software that controls the storage, removal, and use of the data).

- The Program does not move datasets outside of the secured areas for analysis. In the event that such a scenario were to present itself, all data set will be on an encrypted device that is in a locked cabinet in the surveillance area.

Requirement 21. Data transfers and methods for data collection must be approved by the ORP and incorporate the use of access controls. Confidential surveillance data or information must be encrypted before electronic transfer. Ancillary databases or other electronic files used by surveillance also need to be encrypted when not in use.

- The Surveillance Unit uses SEAL Software for the encryption of all potentially confidential information that is sent to CDC. This primarily addresses the upload of Soundex codes to the CDC Secure Data Network for the purposes of 1) duplication review with other state surveillance systems and 2) monthly upload of de-identified cases for national reporting.
- eHARS transfer files are output with encrypted algorithm that meets federal standards. For reporting purposes, CDC uses a soundex code of a person's last name in order to prevent possible identification of any reported individual.
- **Release of Information to the TB Division**
HIV/AIDS patients also infected with TB are reported by designated Surveillance staff to authorized staff of the TB Division of the Arkansas Department of Health. Designated HIV/AIDS Surveillance staff obtain TB case registry data (by line list or diskette) and compare it to HIV and AIDS case data within the HIV/AIDS Surveillance section to ensure confidentiality. Names and HARS state numbers of patients identified who are co-infected with HIV and TB are provided to authorized TB Division staff. The TB case numbers are also obtained by HIV/AIDS Surveillance staff and entered into HARS. This review is conducted on a semi-annual basis. However, information is communicated on an ongoing basis between these Divisions regarding patients who are co-infected.
- **Release of Information to Other Reportable Disease Divisions**
If during surveillance activities other reportable diseases are identified, that information is reported to the authorized staff of the respective divisions

Requirement 22. When case-specific information is electronically transmitted, any transmission that does not incorporate the use of an encryption package meeting the Advanced Encryption Standard (AES) encryption standards and approved by the ORP must not contain identifying information or use terms easily associated with HIV/AIDS. The terms HIV or AIDS, or specific behavioral information must not appear anywhere in the context of the communication, including the sender and/or recipient address and label.

- Standard practice in the Surveillance Unit is to never send identifying information electronically until such time that encryption software is available. Confidential material must not be sent to any other staff, provider, or individual using unprotected or unencrypted electronic mail. This includes email sent within the state email system.

Routine dissemination of summary statistics and reports, with no identifying information, may be transmitted by electronic mail.

Requirement 23. When identifying information is taken from secured areas and included on line lists or supporting notes, in either electronic or hard copy format, these documents must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any information that could easily be associated with HIV or AIDS.

- Identifying information taken from secured areas is for data matching with other ADH programs for the purpose of enhancing surveillance. Only the minimum amount of information needed for matching is used. Examples would include name, date of birth and/or social security number.
- Identifying information may also be taken from secured areas for follow up (i.e., site visits, record reviews) in the field by Surveillance staff. Again, only the minimum amount of information is taken in hardcopy format. Materials are secured in a locked briefcase. When possible, materials that must be left in a vehicle should be placed in a lockable trunk.
- While working off-site, all confidential materials must remain in the possession of Surveillance staff at all times and must not be shared with non-staff persons for any reason. Only the minimum information is taken from secured area; materials are placed in a security briefcase and placed in a locked trunk when material is left in a vehicle; material is always in the possession of a staff member
- On return to the office, paperwork containing sensitive information should be disposed by shredding per security policy, if not longer needed. Electronic document must be erased as well, as described by policy.

Requirement 24. Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the surveillance coordinator.

- Surveillance staff shall travel with confidential information only to perform site visits or other necessary surveillance job functions. All field work should be coordinated in such a way as to ensure efficient use of time and that materials can be returned to the secured Surveillance offices by the end of each business day when possible. Under circumstances that precludes this, the Section Chief or Surveillance Coordinator must be notified.

Requirement 25. Prior approval must be obtained from the surveillance coordinator when planned business travel precludes the return of surveillance information with personal identifiers to the secured area by the close of business on the same day.

- As noted above in Requirement 24, Surveillance staff must make every effort to return confidential information to secured offices by the of each business day. The Section

Chief or Surveillance Coordinator must be notified prior to any overnight travel that must take place.

- Materials should not be taken home unless a prolonged site visit prevents them from being returned to the office. In this case, precautions must be taken at the home to protect the information. Materials shall remain in a heavy-duty locked briefcase until returned to the Surveillance offices for secure storage. All overnight trips has to be approved in advance by the Section Chief, when traveling with personal identifiable information

Requirement 26. Access to any surveillance information containing names for research purposes (that is, for other than routine surveillance purposes) must be contingent on a demonstrated need for the names, an Institutional Review Board (IRB) approval, and the signing of a confidentiality statement regarding rules of access and final disposition of the information. Access to surveillance data or information without names for research purposes beyond routine surveillance may still require IRB approval depending on the numbers and types of variables requested in accordance with local data release policies.

- Access to any surveillance identifiable information for research purposes beyond routine surveillance requires IRB approval and the signing of a confidentiality statement regarding rules of access and final disposition of the information.
- All requests shall be directed to the ORP for direction.
- **Release of information for Research Purposes**

The Section Chief of the HIV/AIDS Surveillance must approve release of HIV/AIDS case

information. These persons ensure that data with numbers less than four are not released. Names or personal identifiers are never released. No other persons within the unit are authorized to release case data.

Requirement 27. Access to any secured areas that either contain surveillance data or can be used to access surveillance data by unauthorized individuals can only be granted during times when authorized surveillance or IT personnel are available for escort or under conditions where the data are protected by security measures specified in a written policy and approved by the ORP.

- Access to confidential surveillance information and data by personnel outside the surveillance unit must be limited to those authorized based on and expressed and justifiable public health need, must not compromise or impede surveillance activities, must not affect the public perception of confidentiality of the surveillance system and must be approved by the ORP.
- Generally, no staff outside the Surveillance Unit is given direct access to surveillance information or data.
- **Physical Access to Computers and Data**
- All case information is entered into microcomputers, which are linked to a LAN network. This network is password protected and accessible by Surveillance staff only. Offices containing computers and diskettes are secured each night, and access to these offices is

restricted to Surveillance personnel requiring access to patient identifiers as part of their job duties. All computers data, backup diskettes and other confidential information are locked in file cabinets within the Surveillance section.

- **Visual Access to Computer Screens and Documents**
- Surveillance staff arranges for and inform other co-workers before outside visitors are escorted into the Surveillance Unit. Computer screens are cleared and all paper files and documents are put away prior visitors entering the restricted section.

Requirement 28. Access to confidential surveillance information and data by personnel outside the surveillance unit must be limited to those authorized based on an expressed and justifiable public health need, must not compromise or impede surveillance activities, must not affect the public perception of confidentiality of the surveillance system, and must be approved by the ORP.

- Access granted to staff outside the Surveillance Unit were described previously in Requirement 27, and are addressed here as follows:
 - Regular data matching activities between ADH programs for the purpose of enhancing surveillance are approved by the Section Chief based upon justifiable need and availability of staff time and resources. Access can only be granted by the Section Chief

Requirement 29. Access to surveillance information with identifiers by those who maintain other disease data stores must be limited to those for whom the ORP has weighed the benefits and risks of allowing access and can certify that the level of security established is equivalent to the standards described in this document.

- The Surveillance Coordinator will consult with the ORP regarding data matches outside of its usual range of function. The ORP will have final approval in this process.

Requirement 30. Access to surveillance information or data for non-public health purposes, such as litigation, discovery, or court order, must be granted only to the extent required by law.

- The Surveillance Coordinator will defer to the ORP and ADH Office of General Counsel in any requests for identifiable information not used for public health purposes.
- Access to surveillance data or information without identifiable may still requires ORP approval depending on the numbers and types of variables required and in accordance with state data release policies. Approval is only given by the Section Chief after the need of justification is determined.

- **Release of Information by Patient Consent**

Patient information may be released if a patient has given written consent by signing an agency-approved release of information form. Any release of information must be reviewed and authorized by these personnel in the following order: 1) The HIV/AIDS Surveillance Section Chief 2) the Branch Chief of the Health Statistics Section, 3) the Director of the Center for Public Health Practice, 4) the Chief Operating Officer of the

Arkansas Department of Health 5) the Department's legal counsel.

- **Release of Information to Court-Appointed Guardians or Executors of Estate**
Patient information may be released if a court-appointed guardian or executor of estate has given written consent by signing an agency-approved release of information form. Any release of information must be reviewed and authorized by these personnel in the following order: 1) The HIV/AIDS Surveillance Section Chief 2) the Branch Chief of the Health Statistics Section, 3) the Director of the Center for Public Health Practice, 4) the Chief Operating Officer of the Arkansas Department of Health 5) the Department's legal counsel.

- **Release of Information to Department of Human Services when Child Abuse is Suspected**
Surveillance staff will report cases involving children under the age of 14 when rape or incest is suspected to DHS, Division of Children and Family Services (DCFS). The

ADH

Policies and Procedures Manual, MCH, Vol. 2, Child Health Section reads that any person who has reasonable cause to suspect a child (under age 14) is being sexually abused to report such suspicions as set out and defined in the Arkansas Criminal Code and its amendments.

Security Breaches

Requirement 31. All staff that is authorized to access surveillance data must be responsible for reporting suspected security breaches. Training of nonsurveillance staff must also include this directive.

- Employee agreements include discussion of possible employment ramifications, as well as criminal and civil liabilities, for any unauthorized disclosure of HIV/AIDS surveillance information and data. All staff must adhere to this requirement

Requirement 32. A breach of confidentiality must be immediately investigated to assess causes and implement remedies.

- Occurrences of both security and confidentiality breaches shall be documented in a security log by the Surveillance Coordinator and investigated by the ORP. Breaches of confidentiality will be investigated by the Section Chief, Sharon Donovan.

Requirement 33. A breach that results in the release of private information about one or more individuals (breach of confidentiality) should be reported immediately to the Team Leader of the Reporting, Analysis, and Evaluation Team, HIV Incidence and Case Surveillance Branch, DHAP, NCHSTP, CDC. CDC may be able to assist the surveillance

unit dealing with the breach. In consultation with appropriate legal counsel, surveillance staff should determine whether a breach warrants reporting to law enforcement agencies.

- For the purposes of this policy, security breaches are defined as those occurrences whereby Surveillance staff has allowed the opportunity for a person to be identified with HIV/AIDS, but confidentiality breach does not necessarily occur.
A confidentiality breach is when a person with HIV/AIDS is identified by the Program against policy. The ORP or Surveillance Coordinator shall promptly report either type of breach to CDC.
- In consultation with appropriate legal counsel, the ORP will determine whether a breach warrants report to law enforcement agencies.

Laptops & Portable Devices

Requirement 34. Laptops and other portable devices (e.g., personal digital assistants [PDAs], other hand-held devices, and tablet personal computers [PCs]) that receive or store surveillance information with personal identifiers must incorporate the use of encryption software. Surveillance information with identifiers must be encrypted and stored on an external storage device or on the laptop's removable hard drive. The external storage device or hard drive containing the data must be separated from the laptop and held securely when not in use. The decryption key must not be on the laptop.

Other portable devices without removable or external storage components must employ the use of encryption software that meets federal standards.

- The Program currently uses only laptop computers primarily to provide presentations of aggregate data, and not for daily surveillance activities that would require personal identifiers.
- Laptops cannot be used for surveillance activities without sound justification and prior approval from the Section Chief. In such a case, data will be password protected and/or encrypted and stored on an external storage device or on the laptop's removable hard drive. The external or hard drive containing the data must be separated from the laptop and held securely when not in use.
- Computers that are no longer of use to the Program will undergo a full wipe, per standards set by the U.S. Department of Defense.
- In no instance should identifiable data be left on a computer workstation C: / drive or laptop. Such data can only reside on 1) eHARS server located at the ADH Data Center, 2) network drive with restricted access, or 3) storage media. Storage media are placed in a locked cabinet within the Surveillance's secured area.

Removable & External Storage Devices

Requirement 35. All removable or external storage devices containing surveillance information that contain personal identifiers must (1) include only the minimum amount of

information necessary to accomplish assigned tasks as determined by the surveillance coordinator, (2) be encrypted or stored under lock and key when not in use and (3) with the exception of devices used for backups, devices should be sanitized immediately following a given task.

- Surveillance activities involving personal identifiers are usually conducted only in the Surveillance Unit secured area. Storage media include floppy disks, CDs, and USB keys; those used for confidential information are clearly marked for such purposes.
- When data is moved between workstations using storage media, they must remain in the secured area, be accounted for at the end of the work day, and then be placed in a locked cabinet.
- Only the minimum identifiable information needed for a given task is placed on storage media. Entire databases are not to be moved without sound justification and prior approval from the Section Chief.
- Identifiable information on storage media will not simply be deleted; they must be reformatted to ensure that data is rendered completely unreadable. If the media will no longer be used, efforts should also be made to physically damage the media prior to disposal.



Arkansas Department of Health

4815 West Markham Street Slot-33 • Little Rock, Arkansas 72205-3867 • Telephone (501) 661-2408

Governor Mike Beebe

Paul K. Halverson, DrPH, FACHE, Director and State Health Officer

HIV/AIDS Surveillance Unit (Center for Health Statistics Registries)

Employee Statement of Confidentiality

As an HIV/AIDS Surveillance (Center for Health Statistics Registries) employee, subcontracted employee, extra-help employee, or other Communicable Disease employee, I understand that I will be exposed to very privileged patient information. The patient's right to privacy is not only a policy of the Surveillance Unit, but is specifically guaranteed by statute and various government regulations.

I understand that intentional or involuntary violation of the Arkansas HIV/AIDS Surveillance Confidentiality and Security Policy is subject to appropriate disciplinary action(s) that could include being discharged from my position and/or being subject to civil penalties or criminal prosecution. By initialing the following statements I further agree that:

_____ I will never discuss patient information with any person outside the Surveillance Unit who is not directly affiliated with the patient's care.

_____ I will handle confidential data, line lists, and lab reports as discretely as possible, and I will never leave confidential information in view of others unrelated to the surveillance activity.

_____ I will secure all confidential information when not in use and shred documents appropriately. I will encrypt or use passwords on all computer files when not in use.

_____ Upon resignation or termination of my position, I am still bound by these policies To protect the confidentiality of the patients in the surveillance database.

I have received, read, understand, and agree to comply with the Arkansas HIV/AIDS Surveillance Confidentiality and Security Policy in the course of my work.

Employee's name (print)

Employee's signature

Date

Section Chief's name (print)

Section Chief's signature

Date



Arkansas Department of Health

4815 West Markham Street Slot-33 • Little Rock, Arkansas 72205-3867 • Telephone (501) 661-2408

Governor Mike Beebe

Paul K. Halverson, DrPH, FACHE, Director and State Health Officer

Arkansas Department of Health

4815 West Markham Street Slot-33 • Little Rock, Arkansas 72205-3867 • Telephone (501) 661-2408

Governor Mike Beebe

Paul K. Halverson, DrPH, FACHE, Director and State Health Officer

HIV/AIDS SURVEILLANCE UNIT (Center for Health Statistics Registries)

Confidentiality Statement Upon Separation

I understand that all patient information related to HIV/AIDS that I have had access to as part of my employment at the Arkansas Department of Health is to remain confidential.

All paper work and/or diskettes with confidential information that I have had access to as part of my employment at the Arkansas Department of Health are in a locked cabinet secured in the Surveillance Unit.

All keys and electronic cards to cabinets and building have been surrendered.

Employee's name (print)

Employee's signature

Date

Surveillance Section Chief (print)

Surveillance Section Chief's signature

Date



Arkansas Department of Health

4815 West Markham Street Slot-33 • Little Rock, Arkansas 72205-3867 • Telephone (501) 661-2408

Governor Mike Beebe

Paul K. Halverson, DrPH, FACHE, Director and State Health Officer

**HIV/AIDS SURVEILLANCE UNIT
(CENTER FOR HEALTH STATISTICS REGISTRIES)**

SEPARATION CHECKLIST

Employee's Name: _____

Date Departed: _____

Date	Action
_____	Reviewed confidentiality issues with employee.
_____	Files and office secured.
_____	Keys to office building, surveillance office, and file cabinets surrendered to: _____
_____	Employee's ID removed from surveillance network system.

Section Chief's name (print) _____

Section Chief's signature _____

_____ Date



Arkansas Department of Health

4815 West Markham Street Slot-33 • Little Rock, Arkansas 72205-3867 • Telephone (501) 661-2408

Governor Mike Beebe

Paul K. Halverson, DrPH, FACHE, Director and State Health Officer

**HIV/AIDS Surveillance Unit
(Center for Health Statistics Registries)**

Staff Access

Staff involved in the HIV/AIDS Surveillance Unit:

Name	Position
1. <u>Jawaski Fisher</u>	<u>Health Services Specialist II</u>
2. <u>Mary Stiles</u>	<u>Health Program Specialist I</u>
3. <u>Marlene Roy</u>	<u>Administrative Specialist I</u>
4. _____	_____

Staff with direct access to HIV/AIDS surveillance data:

1. <u>Keeven Murphy</u>	<u>Health Program Specialist I</u>
2. <u>Cynthia Neal</u>	<u>Health Program Specialist I</u>
3. <u>Sharon Donovan</u>	<u>Section Chief</u>
4. <u>Marie Wilson</u>	<u>Administrative Analyst</u>

Information Technology staff with access to surveillance hardware and data:

1. <u>Warren Bankson</u>	<u>Network Administrator</u>
2. <u>Todd Mercer</u>	<u>Senior Program Analyst</u>

All staff listed above has signed an Employee Statement of Confidentiality Statement.

Sharon Judah Donovan, Section Chief

Date