TEXAS HIV/AIDS SURVEILLANCE PROCEDURE MANUAL

OCTOBER 2011

Contents

Introduction

Case Ascertainment, Follow Up and Reporting
What is Reportable 1-1
Reporting Sources 1-1
Record Searching Cases 1-2
Follow Up 1-3
Completing Case Report Forms 1-4
Data Submission 1-6
Appendixes
Appendix A: Reporting Rules
Appendix B: Flow Chart for Lab Reports Received from Central Office
Appendix C: Lookup File Record Search Utility Help
Appendix D: Medical Record Abstraction Instructions
Appendix E: Disposition Codes
Appendix F: Adult Case Report Form and Instructions
Appendix G: Pediatric Case Report Form and Instructions
Appendix H: STD*MIS Form
Appendix I: Death Report Form
Appendix J: Electronic Data Transfer Instructions

Perinatal Surveillance
General Overview 2-1
Reporting/ Ownership 2-1
Data Collection 2-2
Case Ascertainment 2-2
Other Methods of Case Ascertainment 2-4
Follow Up 2-4

Risk and COPHI
Risk Factor Ascertainment 3-1
Cases of Public Health Importance 3-3
Appendixes
Appendix A: Cases of Public Heath Importance (COPHI) and Protocol 776
Appendix B: Risk Factors
Appendix C: Transmission Category

Case Ownership
Case Ownership Assignment 4-1
Determining Residence at Diagnosis 4-1
Assigning a Stateno 4-4
Maintaining Out Of State Cases 4-5
Prison Cases 4-5
OOJ Cases

Appendixes
Appendix A: Procedures for OOS Requests
Appendix B: TDCJ Unit Names
Appendix C: Map of TDCJ Facilities
Appendix D: Medical Record Abstraction Request Forms

Test Types
Laboratory Testing for HIV/AIDS 5-1
Screening Tests 5-2
Confirmatory Tests 5-2
Other Detection Tests 5-3
CD4 Tests 5-5
Tests Used for Pregnancy and Newborns 5-5
Incidence and VARHS 5-6
Appendix
Appendix A: Revised Surveillance Case Definitions for HIV Infection Among Adults, Adolescents, and Children Aged <18 Months and for HIV Infection and AIDS Among Children Aged 18 Months to <13 Years — United States, 2008

Additional Contractual Requirements
Provider Education 6-1
Active Surveillance 6-1
Monthly and Quarterly Reporting 6-1
Annual Site Reviews 6-2
Appendixes
Appendix A: Monthly Reporting Database Instructions
Appendix B: Site Review Tool

Security Policies and Procedures 7-1
Appendixes
Appendix A: Security Policies and Procedures

Introduction HIV/AIDS Surveillance in Texas

Surveillance is the ongoing, systematic collection, analyses, and interpretation of data (e.g., regarding agents/hazards, risk factors, exposures, and health events), and it is essential to the planning, implementation, and evaluation of public health practice. Texas has conducted HIV/AIDS surveillance for over twenty five years. In 1983, AIDS became a reportable condition in Texas, and the Centers for Disease Control and Prevention (CDC) began funding the Texas Department of Health, Bureau of Epidemiology to conduct AIDS surveillance activities. Initially the Texas AIDS Surveillance unit had only two employees, since then the branch has grown and developed to over 45 employees we have today. AIDS surveillance has also evolved since AIDS was first identified in 1981. Prior to 1993, reportable AIDS cases were defined by opportunistic infections (OI) in conjunction with a physician diagnosis of HIV. As laboratory methods improved, the CDC expanded the case definition of AIDS to include immunological evidence of disease, particularly CD4 test results. In 1994, Texas added pediatric HIV cases among children less than 13 years of age to the list of conditions reportable by name in Texas. During the same year, Texas implemented an HIV reporting system based on unique identifiers for adult and adolescent HIV cases. HIV later became a condition reportable by name in Texas in 1999.

Currently, Texas rules and regulations require that “any specimen derived from a human body that yields microscopic, cultural, serological or any other evidence of AIDS, chancroid, chlamydia trachomatis infection, gonorrhea, HIV infection or syphilis, including a CD4+; T lymphocyte cell count below 200 cells/microliter or a CD4+; T lymphocyte percentage of less than 14%” must be reported to the local health department. Effective January 1, 2010, all CD4+ cell counts and percentages, all viral load test results, and negative PCR results for children less than 4 years of age will also be reportable.

Surveillance staff at local and regional HIV/AIDS surveillance sites across Texas plays an integral role in ensuring the timely and accurate reporting of new HIV/AIDS cases. Though surveillance staff learn of new cases primarily through electronic laboratory reports distributed from the Central Office in Austin, Texas, information about potential new cases also comes from a variety of other sources, including medical providers, routine matching to other registries, and active surveillance. Central Office depends upon surveillance staff to investigate and gather the information required to make cases reportable upon learning about potential new cases. Surveillance, however, does not end with the initial reporting of cases. Surveillance staff is also expected to conduct follow-up to the initial case report to obtain additional and/or missing information. HIV/AIDS case records are not closed until cases die.

Chapter 1 Case Ascertainment, Follow Up and Reporting

The primary goal of the HIV/AIDS surveillance program is to collect and analyze data essential for monitoring the HIV epidemic, planning interventions, and evaluating public health programs. To achieve this goal, surveillance sites must identify potential HIV cases, follow-up on all potential cases, complete case report forms on cases and report all HIV positive cases in a timely and accurate manner. In addition to identifying and reporting new cases, it is critical that all required case information is collected and updated as necessary.

1-1 What is Reportable

Texas law requires the reporting of all HIV and AIDS cases to the local health authority. Additionally, it is required that all laboratory tests performed that yield evidence of HIV, all viral load test results, and all cd4 test results are reported to their local health authority (see *Appendix A: Texas Reporting Rules*).

Because HIV did not become reportable by name in Texas until 1999, not all individuals diagnosed with HIV are reportable in Texas. Persons diagnosed with HIV prior to 1999 who have not had an HIV laboratory test that meets the HIV case definition or physician's diagnosis after December 31, 1998, or have not had an AIDS diagnosis, do not meet reporting requirements and are not reportable in Texas. Such cases will only become reportable in Texas once they receive either an HIV laboratory test that meets the HIV case definition, a physician's diagnosis post-1998, or an AIDS diagnosis. However, once a case meets the above criteria required for reporting, all previous laboratory history, including the pre-1999 information can be reported.

Additionally, persons who test anonymously for HIV are not reportable under Texas law. When surveillance staff receives a previously unreported positive HIV test result, they should contact the provider for follow-up information. If the determination is made that the positive HIV test was performed anonymously, the local surveillance personnel should not take any further action.

1-2 Reporting Sources

Sources of information on HIV cases include hospitals, physicians in non-hospital based practices, public and private clinics, counseling and testing sites, laboratories, insurance companies, case registries (e.g. TB registry, death certificates), and other sources. Surveillance sites should maintain lists of potential sources of information on HIV/AIDS patients in their jurisdiction. This section summarizes the different mechanisms that surveillance sites should use to identify unreported HIV/AIDS cases or receive additional information on a reported case. Subsequent sections address how to follow up on these reports.

A. Lab Reports from Central Office

Daily, Central Office receives lab reports from a number of different laboratories, including several large reference laboratories. These lab reports are received in both electronic and paper format. The paper lab reports are entered into a database in Central Office and combined with the lab reports received electronically, so all lab reports received by Central Office are in electronic format. Central Office processes these

electronic lab reports and distributes them daily over the TxPHIN to surveillance sites based on patient address or provider address if the patient address is not available.

Electronic lab reports are electronically matched to records in eHARS, prior to distributing to the surveillance sites. Any lab reports for individuals who have an existing record in eHARS will have their unique identification number, the State Number (Stateno), added to the lab report before it is transmitted to surveillance sites. See *Appendix B: Flow Chart for Lab Reports Received from Central Office*, for an outline of the process that surveillance sites should follow when receiving these reports from Central Office.

For information on how to receive and view laboratory report, see Appendix K.

B. Lab Reports Received Locally

In addition to the laboratory reports received electronically from Central Office, surveillance sites may receive paper lab reports directly from laboratories in their area. Most hospital-based laboratories report directly to surveillance sites. Since Central Office does not directly receive a copy of these lab reports, surveillance sites must send all lab reports received locally to central office. Surveillance sites must also manually record search these cases to determine if the case has been reported to eHARS and the appropriate follow-up needed for the case**.**

C. Provider Reports

Some providers notify surveillance sites directly by submitting lists of identified HIV/AIDS cases. In addition, some providers may complete case report forms themselves.

D. Case Information from Registry Matches at Central Office

Central Office staff routinely matches the eHARS database to other disease registries to identify potential cases and obtain additional case information on existing cases in eHARS. Any potential cases identified though these registry matches will be distributed to the surveillance sites for appropriate follow-up. The following registry matches are performed on a routine basis.

eHARS is linked to the following registries at least annually:

- STD*MIS
- Texas HIV Medications Program
- Texas Vital Statistics birth and death records
- Tuberculosis
- Social Security Death Index (SSDI)

Central Office may also match eHARS records to registries other than those listed above such as the Birth Defects and Cancer registries. Surveillance sites will be notified of any additional registry matches.

1-3 Record Searching Cases

When information is received from any of the aforementioned data sources, Central Office requires surveillance staff to conduct a record search to determine whether the case has been reported into eHARS. Note that since the lab reports received from Central Office have already been electronically matched to eHARS, the lab reports which contain a Stateno do not need to be record searched. All other reports must be record searched.

Record searches can be done one of three ways: Direct eHARS search, Look-up File Search, or Central Office eHARS search.

Direct eHARS search

The central eHARS database can be searched using a VPN connection. Only surveillance sites that have VPN access are able to search the central eHARS database. For specific instructions on record searching cases in eHARS refer to *Lesson 2.2 of the Introduction to eHARS v3.0 manual*.

Look-up File search

The Look-up File is a database of all living cases reported in eHARS. However, the look-up file only contains the core variables needed to record search a case. This dataset is provided to those areas that have record search needs, but are not able to directly access the central eHARS database. Refer to *Appendix C: Lookup File Record Search Utility Help* for instructions on using the Look-Up file.

Central Office eHARS search

If a site does not have access to either a Look-Up File or central eHARS, staff may contact Central Office via telephone to conduct a record search. When calling for a record search, surveillance staff may leave a message with confidential information if a Central Office staff member's voicemail does not indicate s/he is out of the office. Efforts will be made to complete record search requests within one business day. Note that if you are STD*MIS personnel authorized to call Central Office for record searches and are co-located with a surveillance site with VPN or Look-Up file access, you must do a local record search prior to calling Central Office.

Potential cases should be searched using multiple criteria to ensure that the case has not already been reported with a different name, date of birth, or social security number. When record searching potential cases, at minimum the following criteria should be used:

1. Last Name and First Initial
2. Date of Birth
3. Social Security Number (if available)

If the person is not found in eHARS, then s/he should be considered a potential new HIV/AIDS case and should be investigated as such. If the person is found in eHARS, then it must be determined if the existing case requires any further investigation (e.g. an HIV case needing updating to AIDS or an NIR case needing further risk investigation).

1-4 Follow-up

Surveillance sites <u>must</u> immediately follow-up on <u>all</u> potential new HIV cases that have not yet been reported, by completing a Case Report Form (CRF), including the Testing and Treatment History (TTH) data elements. Surveillance staff <u>must also</u> immediately

follow-up on all reported cases progressing from HIV to AIDS by completing a CRF. Potential new HIV cases include all persons for whom surveillance staff receive confirmatory laboratory tests (i.e., positive western blots or IFAs), detectable viral loads, other HIV detection tests, or documentation from a provider of a diagnosis. Cases progressing from HIV to AIDS include persons with a CD4 count below 200 or CD4 percentage below 14% or the diagnosis of an opportunistic infection.

A medical chart abstraction must be conducted to gather the information required to complete the CRF and the TTH data elements. Medical record abstractions may provide information on previous diagnoses and treatment history, other medical conditions, including opportunistic infections, demographics, and risk factors. Medical record abstractions should be done through a field visit to the provider's facility to ensure that all case information is captured. Telephone abstractions should only be done in extenuating circumstances that would prevent surveillance staff from reporting cases within 45 days or when in-person medical record abstraction visits cannot be performed (for example, when a provider is located at a great distance and there are no other cases in that area or patient is tested by insurance agency). See *Appendix D: Medical Record Abstraction Instructions*, for guidance on conducting medical chart abstractions.

In addition to conducting a medical record abstraction, surveillance staff are encouraged to explore other data sources available to gather information required to report new cases. If there are elements on the CRF that cannot be completed based on the medical record abstraction (e.g. risk) surveillance staff must attempt to obtain the information from additional data sources such as STD*MIS or Disease Intervention Specialist (DIS) notes. Note that information obtained from another data source should be entered onto a new CRF, the information should never be entered onto the CRF used for the medical record abstraction.

If surveillance staff receives non-detectable viral loads, CD4 counts above 200, or CD4 percentages above 14% for persons who have not been reported, follow-up should be conducted by calling the patient's provider to determine if any additional tests have been performed to ascertain the patient's diagnostic status. However, these potential cases should be assigned a lower priority than potential new cases that are immediately reportable.

Surveillance staff should follow locally established protocol for notifying DIS officers of cases when appropriate. See *Appendix E: Disposition Codes*, for information on Disease Disposition, Field Record, and Interview Record Codes that are commonly used by DIS.

1-5 Completing Case Report Forms

Case report forms must be completed for all reportable HIV/AIDS cases within 45 days of learning of the case. Use the Adult HIV/AIDS Confidential Case Report Form (ACRF) (*Appendix F: Adult Case Report Form and Instructions*) to report all adults ≥13 years of age with an HIV infection or an AIDS diagnosis and the Pediatric HIV/AIDS Confidential Case Report Form (PCRF) (*Appendix G: Pediatric Case Report Form and Instructions*) for children <13 years of age with an HIV infection, AIDS diagnosis or who

were perinatally exposed to HIV (i.e.,a child born to an HIV infected mother). The TTH portion of the ACRF must be completed for all newly reported adult (≥13 years of age) HIV cases. In addition to completing an PCRF, surveillance staff must also complete an Enhanced Perinatal Surveillance form for all perinatal exposures (see Chapter 2: Perinatal HIV Surveillance).

A. Completing the HIV/AIDS Case Report Form (adult and pediatric)
Surveillance staff is required to complete a CRF on all cases which are diagnosed or receiving care at a facility in their jurisdiction, including cases which may reside in another jurisdiction. (See Chapter 4 for information on jurisdictional case ownership.) When assigning statenos for those cases, surveillance staff should use statenos from their own jurisdiction. Once the CRF has been completed, surveillance staff should contact the jurisdiction where the case resided at the time of diagnosis to inform the surveillance staff that a CRF has been completed and a stateno has been assigned. Surveillance staff should also file a copy of the CRF with the lab report.

It is expected that all new HIV cases and all HIV cases with an AIDS diagnosis have a completed CRF based on information gathered from a medical record abstraction. However, additional information may be gathered from other sources, and in this case surveillance staff must complete a separate case report form for each source from which the information was gathered. **DO NOT complete a case report form using information from a laboratory report**.

Specific fields on the case report form must be completed in order to be entered into eHARS. Surveillance staff and supervisors should review each Case Report Form to ensure that all required fields are complete before submitting to Central Office for data entry. If any required field listed below is incomplete, the Case Report Form will be returned to the person who completed the form. All case report forms must have the following fields completed:

- Stateno
- Report Status
- Document source
- Report Medium
- Surveillance Method
- Date Form Completed
- Person Completing Form
- Facility where information was obtained (all fields)
- Patient Legal Name
- Patient DOB

In addition, for a case to be reportable and considered complete, the following information must be obtained for all new cases and case updates from HIV to AIDS:

- Patient Sex
- Patient Race
- Patient Residence at Diagnosis (including zip code)

- Facility of Diagnosis Fields
- Lab information/Physician Diagnosis that made person a case
- Vital Status, including date of death if vital status is deceased

However, HIV/AIDS surveillance sites should strive to provide the most complete and up to date information as possible for all reported cases. Surveillance sites should send CRFs immediately after completion.

Please see *Appendix F: Adult Case Report Form and Instructions,* for detailed instructions on completing the Adult Case Report Form.

Please see *Appendix G: Pediatric Case Report Form and Instructions,* for detailed instructions on completing the Pediatric Case Report Form.

An abbreviated version of the Adult Case Report Form has been developed for reporting update information from STD*MIS on an existing case in eHARS. This abbreviated form has been developed to facilitate the reporting of information from STD*MIS. It has a reduced selection of fields, some of which have been pre-completed to meet the specifications set for reporting update information from STD*MIS. However, there are several limitations that must be recognized when using this form. If a case has never been reported to eHARS, the abbreviated ACRF for STD*MIS cannot be used; instead a full ACRF must be completed on the case. Review of STD*MIS does not meet the requirement for a medical record abstraction. Therefore, if a full ACRF is completed from STD*MIS, a medical record review must also be conducted at the facility of diagnosis or care. No laboratory information can be reported on the Abbreviated ACRF for STD*MIS. If there are earlier lab reports in STD*MIS than those received by HIV Surveillance, a medical record abstraction should be conducted at the facility from which those lab reports originated. This form should also not be used to report clinical information that was collected on patients who were diagnosed in the health department. Instead surveillance staff should review the patient's medical records at the health department and complete a full ACRF based on the medical record review.

Please see *Appendix H: Abbreviated ACRF for STD*MIS Form and Instructions,* for detailed instructions on completing the Abbreviated Adult Case Report Form for STD*MIS.

B. Completing the TTH data elements on the Adult Case Report Form

Surveillance sites are **required** to complete the TTH portion of the ACRF for all newly-reported Texas HIV cases (including persons with HIV who are diagnosed with AIDS concurrently). This information should be reported to Central Office as part of the ACRF. The TTH data elements have been incorporated into eHARS and should follow the same document based principles that are used for reporting information on the ACRF; namely, only information from a single source is reported on an ACRF. For example, when conducting a medical record abstraction at Facility A, only information (including the TTH data elements) found during the medical record abstraction at Facility A is reported

on the ACRF. Additional TTH information should be gathered from other sources, and in this case surveillance staff must complete a separate case report form for each source from which the information was gathered.

If there is documentation at the time of diagnosis that the case was previously diagnosed and reported in another state then an Out of State record search request HIV/AIDS Request Form should be completed (See Chapter 4, Appendix A, Procedures for OOS Request). If it is determined that the case has not been reported in another state and is a Texas case, then complete the ACRF including the TTH data elements following the same procedures as you would use for any new case.

All ACRF forms received at Central Office will be reviewed for accuracy and completeness. Central Office will review TTH data elements to verify that all questions were answered and that the information on the form did not come only from a laboratory report. Incomplete or inaccurate forms will be returned to the submitting site to be redone.

Central Office will generate monthly reports and distribute them to each surveillance sites. Please refer to Chapter 6 for more information on monthly reports.

C. Completing the Death Report Form

The death report form has been created so that surveillance sites can provide updated death information on existing cases found in one of the following four sources: a coroner's database, an individual death certificate, the Social Security Death Index (SSDI), or your local Vital Statistics office. If death information is discovered during a medical records abstraction, that information should be included on the CRF and not separately reported on a Death Report Form. It is important to note that cases cannot be reported for the first time using the Death Report Form. There must be some type of clinical indication of HIV/AIDS diagnosis for a case to be reportable. See Appendix I for the Death Report Form and Instructions.

1-6 Data Submission

Surveillance staff must submit Case Report Forms for data entry and other necessary documentation to Central Office <u>at least once a week</u>. Submissions are due to Central Office by Friday of each week. It is recommended that a supervisor review all CRFs prior to submission to Central Office. Surveillance sites should retain copies of all forms submitted to Central Office. For surveillance sites that have scanning capabilities, *Appendix J: Electronic Data Transfer Instructions* outlines how to encrypt, zip, and upload data for electronic submission. For sites that are not able to transmit data electronically, documents must be sent using the mail service using the following procedures:

- Double envelope all mail with each envelope marked "CONFIDENTIAL" and "TO BE OPENED BY ADDRESSEE ONLY" .
- Do not include the words HIV/AIDS/STD in the body of the address or return address. This applies to any address stamps and pre-addressed envelopes.
- Address the package as follows:

- For **ANY** packages that are going through USPS, including USPS priority mail, USPS express mail, and USPS first class mail, use the below address:

  STANLEY SEE
  EPIDEMIOLOGY AND SURVEILLANCE BRANCH
  TEXAS DEPARTMENT OF STATE HEALTH SERVICES
  PO BOX 149347
  AUSTIN, TX 78714-9347

- For mail sent using UPS, FEDEX, another overnight method, or mail delivered by courier use the address :

  SURVEILLANCE: STANLEY SEE
  DEPARTMENT OF STATE HEALTH SERVICES (DSHS)
  4110 GUADALUPE STREET
  BLDG. #636
  AUSTIN, TX 78751

Confidential information should never be sent using facsimile transmission.

Appendix A:
Texas Reporting Rules

Texas Reporting Rules

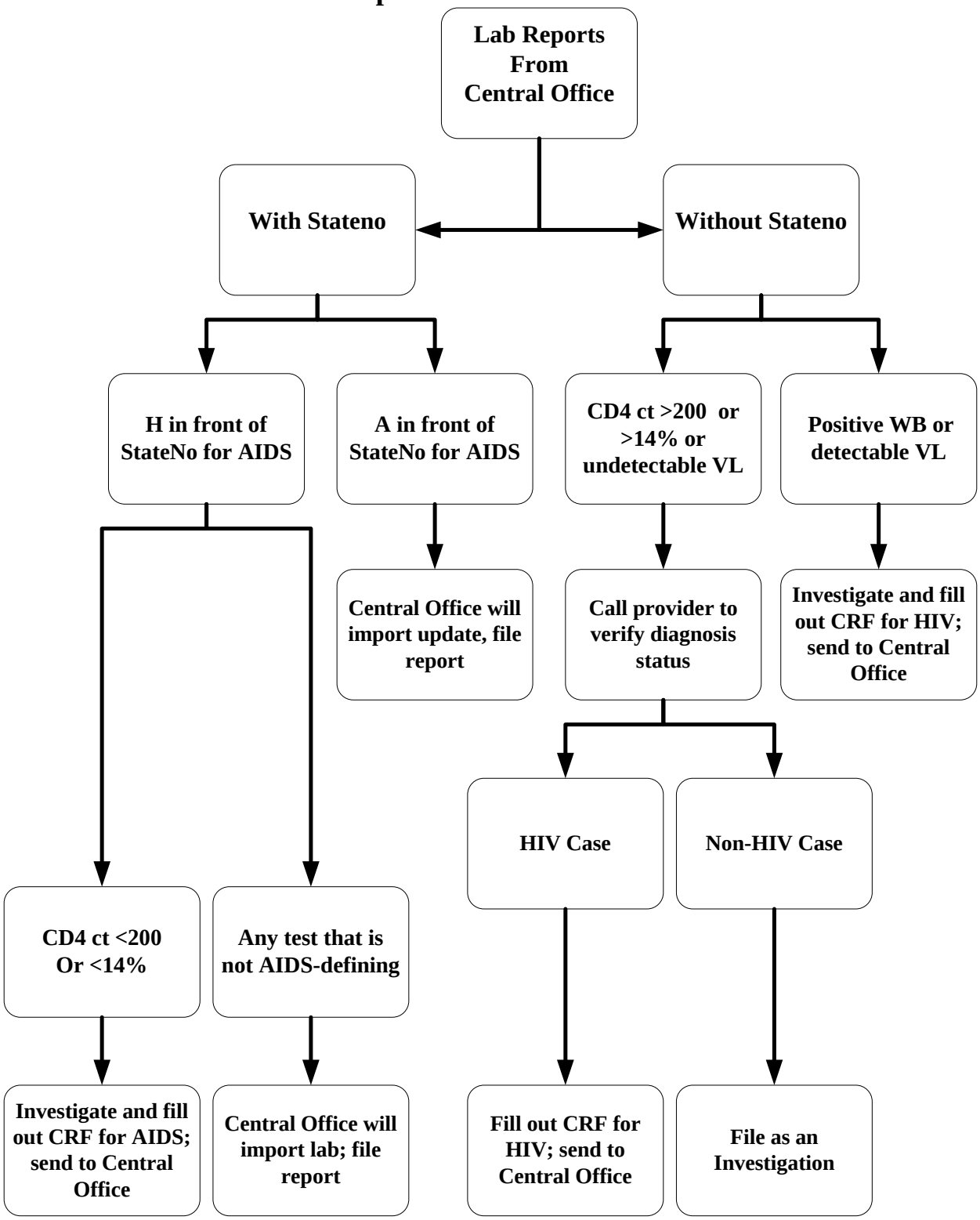
Complete and accurate HIV/AIDS and Sexually Transmitted Disease (STD) reporting by healthcare providers and laboratories is critical in order to monitor disease burden and track changes in these diseases in Texas. Texas law mandates the reporting of HIV/AIDS and STD by both healthcare providers and laboratories and Texas Administrative Code, Chapters 97.131-97.134 specifies the reporting process for HIV/AIDS, syphilis, gonorrhea, chancroid and Chlamydia. Communicable disease reporting is exempt from HIPAA (Health Insurance Portability and Accountability Act of 1996).

Texas Administrative Code can be found at the below website:
http://info.sos.state.tx.us/pls/pub/readtac$ext.ViewTAC?tac_view=5&ti=25&pt=1&ch=97&sch=F&rl=Y

In addition, the below website provides additional information on Reporting:
http://www.dshs.state.tx.us/hivstd/healthcare/reporting.shtm

Appendix B:
Flow Chart for Lab Reports Received from Central Office

Flow Chart for Lab Reports Received from Central Office



*If you receive a stateno that begins with a "U", this is an OOS case that needs to be record searched with the other state to determine current case status.

Appendix C:
Lookup File Record Search Utility Help

Lookup File Record Search Utility Help

Introduction

In an attempt to reduce the number of phone calls made to conduct record searches and the numerous work hours that this consumes for both surveillance staff and Central Office staff, an eHARS Record Search Utility has been developed. To keep the size of this file manageable, it has been limited to a subset of the eHARS data - it contains reported HIV/AIDS cases in eHARS and just those fields that will be useful to see when conducting a record search.

To Search By Name

Names in the look-up file are in the format LName, Fname Mname and may be followed by additional names such as AKAs and nicknames. The search will be conducted on the exact text entered into the box and locate it anywhere in the name field. Enter only as much of the name as you are sure of, using the comma to control searching in the last name or first name positions or both. Because of inconsistencies in data entry it may be helpful to search only on first or last name if they are sufficiently unique to avoid a huge result list. **Wildcard searching is also available. An asterisk will substitute for any number of unknown characters and a question mark will substitute for any unknown single character.**

For example, entering: Johnson, Bill - yields all records with that name, including AKAs if entered with the 'LName, FName' format

Johnson, - yields all records with the last name Johnson

, Bill - yields all records with the first name Bill

J*son - yields all records with names like Johnson, Jackson, Jason, etc.

Johnson, ?ill - yields all records with the last name Johnson and the first names like Bill, Willy or William (to further limit results to only first names like Bill or Will use a space and asterisk at the end - , ?ill *)

To Search By Birth Date

Remember that the eHARS date format is MM/DD/YY. This is actually a character string search like the name search, so enter as much of the date as you are sure of and you can use wildcards for the rest.

For example, entering: 12/15/77 - yields all records with that exact birth date

12/*/77 - yields all records from Dec. 1977

12/1?/77 - yields all records from Dec. 10-19, 1977

12/ - yields all records with 12 as the month or the day

To Search By State Number

Stateno's generally follow a pattern of a one or two letter prefix, followed by a 5 to 8 digit number; however there are statenos with no prefix. When searching by Stateno don't use any spaces. Wildcard searches with the * and ? are available.

To Search By Social Security Number

When searching for a case by SSN, enter SSNs without any spaces or separators. Keep in mind that SSNs are frequently missing or only a portion of the number may have been entered, such as the last four digits. Wildcard searching with the * and ? are also available - use question marks to control for digit position.

For example, entering: 123456789 - yields all records with that exact SSN
123 - yields all records that contain the numbers 123 in sequence anywhere in the SSN
?????6789 - yields all records with 6789 as the last four digits of the SSN

To Search By All Criteria Simultaneously

Enter as much text as you wish in the Name, Birth Date, Stateno and SSN boxes as described above and the search will return cases that meet all criteria.

Results

Results will be displayed in a separate window along with a number of fields that may be of use for quick record searches. The “OOS?” column indicates whether the case came from the Out of State database rather than eHARS. For further case details, click the Detail button on the right side of the Results window to open a second window with more information about the individual. Close the Detail and Results windows to return to the search page.

Clear Form For New Search

Click the “Clear Form For New Search” button to clear all the search boxes and reset the form for a new look up.

Appendix D:
Medical Record Abstraction Instructions

Medical Record Abstraction Instructions

How to Initiate an Abstraction Visit

If surveillance staff have never visited a facility, they should initially contact the facility by sending a letter to the facility's Health Information Management Director 2-3 weeks prior to the visit. The letter should include a request for a list of patients with HIV/AIDS ICD-9/10 codes in the primary and secondary diagnoses positions who received services at the facility during a specified time frame. See Figure 1 for an example letter requesting medical chart access. For pediatric exposures, surveillance staff must request the labor, delivery and birth records to ensure that all necessary records are obtained.

TEXAS DEPARTMENT OF STATE HEALTH SERVICES

DAVID L. LAKEY, M.D.
COMMISSIONER

1100 W. 49th Street • Austin, Texas 78756
1-888-963-7111 • http://www.dshs.state.tx.us
TDD: 512-458-7708

September 18, 2007

Presbyterian Hospital
1105 Central Expressway N
Allen, TX 75013

ATTN: Donna Ballard, Infection Control

The Texas Department of State Health Services, HIV/AIDS Surveillance Program is charged with collecting information on communicable diseases. The Texas Health and Safety Code, Chapter 81, section §81.041 states "Acquired Immunodeficiency Syndrome and Human Immunodeficiency Virus infection are reportable diseases under this chapter for which the board shall require reports." The HIV/AIDS Surveillance Program is responsible for carrying out this mandate. We need and require your cooperation in collecting accurate information.

One of the required functions of the surveillance program includes retrospective record reviews, which focus on gleaning unreported HIV/AIDS cases, providing updated information on diagnostic status, missing demographic information, risk factors, laboratory and clinical data, death updates as well as assessing the quality and validity of information collected as it existed in the source file when the record/case was initially reported. These reviews are historically to be done at a minimum once a year and preferably on a quarterly based on the number of case reports per facility. This information is generally found in the medical record in the demographic face sheet, physician progress notes, nursing notes, History & Physical, Physician Consultations, any and all laboratory reports including pathology, radiology and reference laboratory reports, social work notes and the discharge summary. The information obtained is kept strictly confidential. A chart memo will be placed in the record once reviewed to meet HIPPA guidelines.

An Equal Employment Opportunity Employer and Provider

Figure 1

The State and Local Health Department are exempt from certain aspects of HIPPA as it pertains to reporting of communicable diseases. Please note sections 164.512 (a) & (b) of the Texas Heath and Safety code are the sections which allow us the right under HIPPA to review the records requested without restriction. Additionally the following sections in the Rules and Regulations Governing Control of Reporting of Notifiable Conditions for the state of Texas permit record reviews for the stated purposes. Please reference sections §97.8 (A) & §97.10 (A)–(C)

I would like to request all medical records coded with ICD 9, 042 Primary and Secondary diagnoses, and V08 asymptomatic, as well as any of the charts of the children born to women with the afore mentioned codes, on the premises from January 2006 trough September 2007. I will also have Viola Arevalo from the Department of State Health Services join me for technical assistance during our visit. We would like to review these records on October 10th, which is 3 weeks from now if agreeable.

Should you have any questions regarding surveillance activities or reporting requirements, please feel free to contact me (817) 264-4773 or the Communicable Disease Program manager Gary Willett at (817) 264-4771.

Sincerely,

Valerie Carson
HIV Surveillance Specialist
Health Service Regions 2/3

An Equal Employment Opportunity Employer and Provider

Figure 1 (continued)

Reviewing Records

Staff should become familiar with the facility where medical records are being viewed, as some facilities may have multiple satellite offices and records may not be stored at the main facility. Medical records from the following types of facilities typically have the information necessary to complete case report forms:

- Inpatient
- ER
- Outpatient labs/radiology/pathology
- Labor and delivery
- Prenatal
- HIV Clinical
- Infant delivery record (birth record)
- EMS run reports (for cases brought to the hospital by ambulance)

The following items should be obtained whenever possible when abstracting:

- Race
- Sex
- Origin of birth
- Date of birth
- Social Security Number (SSN). We can not ask the provider to supply us with the SSN, but it can be noted during a medical record review.
- Names of sex partners
    - All named sex partners should be record searched in HARS and STD*MIS
    - Any partners found in HARS will be cross referenced in comments so risk may be updated or validated.
- Risk
- Earliest EIA/WB
- Earliest CD4 T-lymphocytes. Ensure that you do not lose or overwrite the first AIDS defining CD4 count.
    - CD4 count below 200 or 14%
- Earliest Viral loads
    - Qualitative: negative or positive
    - Quantitative: has a numerical value; ensure that you do not lose or overwrite the first detectable viral load after the year 2000
- Any opportunistic infections (refer to Appendix A in Chapter 6 for information on reportable Opportunistic Infections)
- Pregnancy
    - Note if pregnancy is indicated and follow until birth of the child. Each site will develop a procedure and/or tracking system for following pregnant HIV+ women.
    - Documentation of negative tests during pregnancy or at labor and delivery should be recorded for women who seroconvert after their initial negative test.
    - Documentation of CD4 counts and Viral Loads during pregnancy/labor and delivery/ and 6 months postpartum should be recorded.

The following portions of a medical record are useful in obtaining information to complete fields on the CRF. To be considered a complete abstraction, surveillance staff must be reviewed (when available):

- Intake forms
  - Race
  - Sex
  - Country of origin
  - Date of birth
  - SSN
- History and physical
  - Risk
  - AIDS related complexes
  - Indication of out of state diagnosis/treatment
- Discharge summaries
  - Risk
  - AIDS related complexes
- Laboratory reports/Test results
  - EIA/WB
  - Viral loads
  - CD4's
  - AIDS related viral infections
  - AIDS related bacterial infections
  - AIDS related parasitic infections
- Pathological reports
  - AIDS related cancers
  - AIDS related brain lesions
  - AIDS related bacterial infections
- CT/MRI/X-ray reports
  - AIDS related cancers
  - AIDS related brain lesions
  - AIDS related bacterial infections
- Social histories
  - Risk
  - Transgender reassignment
  - Indication of out of state diagnosis/treatment
- Social worker notes
  - Risk
  - Transgender reassignment
- Case manager notes
  - Risk
  - Transgender reassignment
- Nursing Notes
  - Risk
  - Additional information from patient discussions with the nurse
- Medical Administration records
  - Includes medications patient received

- Physician Progress Notes
    - Risk
    - Diagnosing information

Appendix E:
Disposition Codes

Disease Disposition Codes

100	Chancroid
200	Chlamydia
300	Gonorrhea (uncomplicated)
350	Resistant Gonorrhea
400	Non-Gonococcal Urethritis
450	Mucopurulent Cervicitis
490	Pelvic inflammatory Disease (Syndrome)
500	Granuloma Inguinale
600	Lymphogranuloma Venerium
700	SyphilisReactor
710	Primary Syphilis
720	Secondary Syphilis
730	Early Latent Syphilis
740	Latent Syphilis, Unknown Duration
745	Late Latent Syphilis
750	Late Syphilis with Symptomatic Manifestations
760	Neurosyphilis
790	Congenital Syphilis
800	Genital Warts
850	Herpes
900	HIV
901	HIV Previously Reported
950	AIDS

STD Disposition Codes

A	Preventive Treatment
B	Refused Preventive Treatment
C	Infected, Brought For Treatment
D	Infected, Not Treated
E	Previously Treated for This Infection
P	Not Infected
G	Insufficient Info to Begin Investigation
H	Unable to Locate
J	Located - Refused Examination/Treatment
K	Out of Jurisdiction
L	Other HIV disposition Codes
1	Previous Positive
2	Previous Negative - New Positive
3	Previous Negative - Still Negative
4	Previous Negative - Not Retested
5	Not Previously Tested -New Positive
6	Not Previously Tested - New Negative
7	Not Previously Tested -Not Tested Now
G	Insufficient Information to Begin Investigation
H	Unable to Locate
J	Located - Refused Counseling /Testing
K	Out of Jurisdiction
L	Other

Partner Codes

P1	Sex Partner
P2	Needle Sharing Partner
P3	Both

Cluster Codes

S1	Suspect 1	**A1**	Associate 1
S2	Suspect 2	**A2**	Associate 2
S3	Suspect 3	**A3**	Associate 3

Appendix F

(ACRF not included. Please contact your local HIV Surveillance program to request information about the case report form)

Instructions for Completing the ACRF

Report status

- Check the appropriate status of the report. This a required field on all documents.

Report Status	Description
New Case	An ACRF for a case that has never been reported in eHARS. A new case can be a newly reported HIV (non-AIDS) or a concurrent diagnosis for HIV and AIDS.
Update to AIDS	An ACRF for an AIDS diagnosis of a case that has been reported to eHARS with only an HIV diagnosis.
Other Update	An ACRF containing updated information on an existing case in eHARS.

TDCJ Case

- Check the box for cases known to be in a TDCJ facility at the time of ACRF completion.

Stateno

- If the ACRF is for a "New Case", assign a unique stateno.
- If the ACRF is for an "Update to AIDS" or "Other Update", fill in the eHARS stateno which has already been assigned.
  - **NOTE**: The eHARS stateno should be used for ALL "Update to AIDS" cases – even if the case is progressing from HIV to AIDS in a different jurisdiction. "Update to AIDS" cases will not be assigned a new stateno, even if the case was diagnosed with AIDS in a different jurisdiction.

I. Form Information

- All information in the form section of the ACRF must be filled out to be considered a complete report.

Document Source

- The source from which the information on the ACRF was gathered.
  - An ACRF can only have **one** document source. If you attain information on a case from multiple sources, then you must complete a separate ACRF for each of the sources.
  - Only the information gathered from a particular document source should be used to complete the ACRF (i.e., an ACRF should not contain information from more than one source).
- Use the document source codes provided by the CDC to complete this field. The most common document source codes are listed below. A full list of document source codes can be found in *Appendix 1: Document Source Codes*.
  - If you are unsure which document code to use, please contact Central Office for guidance.

Most common sources:

Source Code	Description
A01.01	Inpatient Hospital
A01.02	Inpatient VA
A02.02	Outpatient VA
A02.03	Outpatient Private Physician
A02.04	Outpatient Adult HIV Clinic
A02.05	Outpatient Infect Disease Clinic
A02.06	Outpatient County Health Depart Clinic
A02.25	Outpatient Hospital
A04.01	Blood Bank (Plasma Center)
A04.05	HIV Counseling, Testing Site
A04.11	STD Clinic
A04.12	DIS Notes (reviewed actual notes)
A06.24	STD*MIS (looked case up in database)
A07.01	Prison, Jail, Other Correctional Facility

Report Medium

- The medium through which you learned about the case. See the table below for selecting the appropriate report medium.

Report Medium	Description
Field visit	Medical record abstraction performed at the facility
Mail	Facility directly mailed information
Phone	Spoke to facility over the telephone to gather information
Electronic Transfer	Information transferred electronically (e.g. RIDR or info on an FTP site)
Disk-CD	Information transferred to site via portables media (e.g. cd)

- If STD*MIS is the source of the information on the ACRF, select "paper form, field visit" as the report medium

Surveillance Method

- The method through which you learned about the case.
- Selecting the appropriate surveillance method is extremely important because this variable is used in the national evaluation plan. See the table below for a description of each of the surveillance methods.

Surveillance Method	Description/Example
Active	You INITIATE a process to obtain a report or gather information. For example, you go to a facility and ask for a list of all of their HIV patients, and in doing this, you learn of a new case.
Passive	You receive a report WITHOUT specifically requesting it. For example, a facility calls you to report a new case. Note that this information must be unsolicited (i.e. you did not call the facility about the case first)
Follow-up	You actively gain information because of a prior report. For example, you call a facility in order to gain more

	information on a case that you received a lab document for.
Re-abstraction	Not to be used at this time
Unknown	You should always know how you learned about a case, so only under rare circumstances should you select unknown

Note that the surveillance method for most cases will be "Follow-up," because surveillance staff generally learn about most cases through lab reports; thus, the completion of the ACRF is a follow-up to the lab report

Date Form Completed

- Enter the date on which you completed the ACRF.

Person Completing Form

- Enter the name of the person completing this ACRF.
  - For surveillance staff, enter your three letter initials only (e.g. MRF). If surveillance staff do not have a middle initial, enter the first and last initial, separated by an underscore (e.g. M_F).
  - For staff who are not surveillance staff (e.g. staff at a clinic), enter your entire name (Last Name, First Name) including your credentials (e.g. MD).

Facility where Information was obtained

- Enter the name of the facility from which the information was gathered, including the corresponding facility type.
  - You must use the exact facility name listed on the excel spreadsheet, which was provided to you by Central Office
  - Please refer to the facility of diagnosis section (VII. Facility of Diagnosis) below for specific instructions on completing facility name fields, including facility type and facility setting, using the list provided by the Central Office.
- If you gathered the information from STD*MIS, refer to your facility list to identify the correct facility name to enter in this field

II. Name

Name Type

- Select the appropriate name type for each name completed and complete the full name of the case. See the list below for available name types.
- For a "New Report", the legal name must be on the form.

Name Type	Description
Legal	Person's legal name
Alias	Person's assumed name
Maiden	Person's name immediately before a first marriage; in most cases, equal to birth name
Married	Name assumed from a partner in a marital relationship
Nickname (Call me)	Person's preferred name when directly addressed, such as a nickname or street name
Birth	Person's name at birth
License	Person's name when granted a license to practice a profession or when issued a formal certificate

Display	The name displayed in a system (for example, a hospital's medical records system) as the primary name for a patient
Indian/Tribal	Person's Indian, indigenous, or tribal name
Professional	Person's professional name, such as a pseudonym or pen name, or an abbreviation of a professional organization or title entered in the Suffix field
Religious	Person's religious name instead of a secular name
Record	Person's officially written and preserved name on record, such as in judicial proceedings

Name

- Include all available name parts (first, middle, last, prefix, and suffix). Spell the name exactly as it appears in the document source, including any punctuation like dashes (-) or apostrophes ('').
- If there are more than two names in one document source, list the additional names and their corresponding name type in the Comments section.

III. Current Address

Address Type

- Select the appropriate address type for the most current address listed in the document source being reviewed. Below is a list of address types available in eHARS.

Address Type	Description
Residential	Address of a residence
Correctional	Address of a correctional facility (including jails)
Homeless	Address of a location where a homeless person spends most of their time. Homeless should only be used with documented evidence that the patient is homeless and not because an address could not be found.
Foster home	Address of a foster home
Bad address	Address is known to be for a place that does not exist.
Postal	A PO box address or the address of a mail receipt facility
Residence at death	Person's residence at time of death
Residence at birth	Person's residence at time of birth
Shelter	Address of a shelter
Temporary	Address of a short term (temporary) residence

Address

- Enter the patient's most current address listed in the document source being reviewed. Be sure to enter the patient's complete address, including street address and zip code.
- If the patient is homeless, record the zip code for the where the person spends most of their time. If this information is not available then enter the zip code for where the person was tested.

- Since eHARS can accommodate more than one address, if a patient has a temporary address or is only temporarily residing in a shelter or correctional facility you should also record the patient's residential address if available. Additional addresses should be recorded in the Comments section, including the address type.

IV. IDs

- List all patient IDs and corresponding ID type. List any additional IDs in the comments section, including the type of ID.

ID Type

- Select the appropriate ID type. Below is a list of ID types available in eHARS.

ID Type
Medical Record Number
OOS Stateno
Prison Number
RVCT (TB) Number
Social Security Number (SSN)
Social Security Number Alias
STD*MIS Number

- For OOS (out of state) cases, include the two letter abbreviation of the other state in the ID type field "other." Use the format <two letter state abbreviation> stateno (e.g. "LA stateno").

ID

- Enter the full ID for each ID type selected.

V. Demographic Information

Diagnostic status

- Select the diagnostic status of the case.

Sex at Birth

- Select the sex of the patient at birth. If the patient's current sex is different than their sex at birth, note this in the Comments section.

Date of Birth/Alias Date of Birth

- Enter the patient's date of birth as it appears in the document source. If the date of birth is known to be an alias date of birth, then complete the alias date of birth field with this date of birth.

Country of Birth

- Check the appropriate box. For cases not born in the USA, write in the full name of the country of birth.

Vital Status/Date of Death/St of Death

- Check the appropriate vital status box. If the case is deceased, the date of death and state of death fields must be completed. Use the state's two letter abbreviation. Use the code "FC" (foreign country) for cases whose place of death is outside of the United States. Refer to *Appendix 2: State Abbreviations* for a list of the two letter state codes.

Ethnicity

- Check the appropriate box. If ethnicity cannot be found, then select "Unknown."

Race

- Check the appropriate box or boxes. If race cannot be found, then select "Unknown."

Extended Race

- If you know the extended race of a case then complete this field using one of the extended races listed in *Appendix 3: Extended Races*.

VI. Residence at Diagnosis

HIV Residence

- Complete the HIV residence section if the ACRF is for a new HIV diagnosis (including concurrent* HIV and AIDS diagnoses).
- The HIV residence address should be the residence where the patient was living at the time of HIV diagnosis.
- Select the "Same as current add." box if the patient's residence at HIV diagnosis is EXACTLY the same (including street address) as their current residence (Section III.). If the HIV diagnosis residence is not exactly the same as the current address complete all fields in this section. Do not select "Same as current address" if current address is not listed on the ACRF.

AIDS Residence

- Complete the AIDS residence section if the ACRF is for a new AIDS diagnosis (including concurrent* HIV and AIDS diagnoses).
- The AIDS residence address should be the residence that the patient was living at the time of AIDS diagnosis.
- Select the "same as current add." box if the patient's residence at diagnosis is EXACTLY the same (including street address) as their current residence (Section III.). Select the "Same as HIV" box if the patient's residence at AIDS diagnosis is EXACTLY the same (including street address) as their HIV residence. If the AIDS diagnosis residence is not exactly the same as the current address or the HIV residence address complete all fields in this section. Do not select "Same as current address" if current address is not listed on the ACRF.

VII. Facility of Diagnosis

- Complete the HIV Diagnosis fields for new HIV diagnosis reports. For new AIDS diagnosis reports, complete the AIDS Diagnosis fields. For concurrent* diagnoses, check "Same as HIV Facility" if the AIDS diagnosing facility information does not differ from the HIV diagnosing facility information.
- Complete the HIV and AIDS facility of diagnosis fields using the list supplied by the Central Office. You must use the exact facility name and corresponding facility type listed on the excel spreadsheet. This list will periodically be updated and distributed to HIV/AIDS surveillance staff at the local and regional health departments.
- The list consists of the facility's ID number as it is stored in eHARS, facility name, city, state, and facility type. The spreadsheet is organized by HIV/AIDS reporting site; to navigate to the different sites, click on the arrows located at the lower left hand corner of the spreadsheet.
    - Because facilities may have more than one Facility Type assigned, be certain to select the facility name with the correctly associated facility type from the search results. For example, JPS HOSP has more than one facility type associated with it, including Inpatient Facility/Hospital, Outpatient Facility/Hospital, and Emergency Room. Please refer to the facility type list located in *Appendix 4: Facility Types* for the complete list of facility types.
    - If the combination of the facility name, city, state and type cannot be found on the list, indicate that the facility needs to be added to the list by checking

* Concurrent Diagnosis is defined as AIDS diagnosis within one calendar month of HIV diagnosis

the 'New Facility' box. **NOTE**: If you come across a facility on the list that is not listed with the facility type you are looking for, then indicate that it is a new facility.

- For out-of-state facilities, complete the facility of diagnosis field with OOS and the two letter abbreviation for the state. For example, if the facility of diagnosis is in Louisiana, then the write "OOS LA" in the facility of diagnosis field. Complete the State field and leave the remaining address fields blank, including City. For Facility Type, write 'Unknown' in the Other field.
  Similarly, for foreign country facilities, complete the facility of diagnosis field with OOC and the two letter abbreviation for the country. Country abbreviations can be found at this website: http://www.worldatlas.com/aatlas/ctycodes.htm
  Leave the address fields blank and write 'Unknown' in the Other field under Facility Type.
- For insurance companies, refer to the facilities list to identify whether this insurance company has been added to eHARS. If this insurance company is new to the facility list, check "New Facility", complete the name of the insurance company and write "INSURANCE SCREENING" in the Other field under Facility Type.
- For Private Physicians, Central Office will no longer use PVT PHYS and the regional designation. Physician names will be entered in the following format: PVT-LName, FName Credential. For example, Dr. Joe Smith MD, would be entered as follows: PVT-Smith, Joe MD
  Complete the city and state information, and select Private Phys for the type.

VII. Personal History

- Complete all questions of the personal history section by selecting "Yes", "No" or "Unknown".
- Select "Yes" if you find documented evidence in that document source that the person has that risk factor.
- Select "Unknown" if the personal history is truly unknown after reviewing all of the information in the document source.
- Only select "No" if you find documented evidence that the person does not have the risk factor (e.g. the medical record states "patient has never injected drugs").
- If you select received clotting factor, complete the clotting factor type and date received.

Heterosexual Relations with any of the following

- This section should only be completed if the case has had documented heterosexual contact. For male cases, you must have checked "yes" for sex with female. For female cases, you must have checked "yes" for sex with male.
  - **For males, you should NEVER select "Yes" to "Heterosexual contact with a bisexual male", since this biologically infeasible.**
- Only select "Yes" to the last four options in the Personal History section if this risk factor might be the primary mode of HIV exposure for this case. In other words, you should select "Yes" to these four questions, if the case is believed to have acquired HIV through one of these risk factors. For example, if a case reports that they report that they had a blood transfusion, but they are a known MSM then you would not respond to the transfusion question. Selecting one of these risk factors will initiate a COPHI investigation.
- Do not select "Yes" to the blood transfusion or transplant questions if the transfusion or transplant occurred outside the United States.
- Only select "Yes" for Worked in a health care or clinical laboratory setting if this was the primary mode of transmission. If the patient is not believed to have acquired HIV through their healthcare work then you should not select "Yes" to this risk factor..

IX. Lab Tests

- All tests marked in this section should be tests that are documented by the source from which you are gathering the information.
  - You should never complete the lab information section using self-reported information
- If you are unfamiliar with a particular test, please refer to Chapter 5 of the manual or call Central Office for further guidance.
- Document additional tests in the comments section.

1. HIV Antibody Tests at Diagnosis

- This section should be completed with only antibody tests done at the time of HIV diagnosis. In other words, if a person had two Western Blots you should only record the Western Blot that was performed at the time of HIV diagnosis.
- Be sure to correctly select whether an HIV Antibody is an HIV-1, HIV-2, or HIV 1/2.

2. HIV Detection Tests

- For this section, you should document all detection tests performed on the patient.
- Note that the *HIV-1 RNA PCR (Qual)* test is a qualitative PCR test (i.e. there is not a numeric result for this test only positive or negative). The RNA PCR test for which there is a numeric result (including results with a "<" or ">" result) is a viral load and should be recorded in section 4. Viral Load tests.
- A **NAAT test** is a qualitative detection test that can be used as a confirmatory test for HIV and so the results from this test should be recorded in this section. Record the results for this test in this section under *HIV-1 RNA PCR (QUAL)*.

3. Immunologic Lab Tests

- For this section you need to record both the first CD4 count/percent performed on the patient and the most recent CD4. If the most recent and the first are same test then record both in the appropriate sections.
- If there are any additional CD4 counts/percents, record these in the comments section of the ACRF.

4. Viral Load Tests

- For this section you need to record only detectable viral loads. Because only one viral load test can be entered for each ACRF, record any additional viral load tests or non-detectable viral loads in the Comments section of the ACRF.
- Be sure to select the correct type of viral load test when recording the results. If you need help selecting the correct test please refer to Chapter 5 of the manual or contact Central Office for guidance.

5. Last documented Negative HIV test

- Enter the last documented negative HIV test on this case, and specify the type of test and date of collection for this test.

6. If HIV laboratory tests were not documented, is HIV diagnosis documented by a physician

- If there are no laboratory tests documented in the source, then you must select "Yes" or "No" in response to whether or not an HIV diagnosis was documented by a physician. You should only select "Yes" if the doctor explicitly stated that the patient is HIV positive. You should not select "Yes" if the person's HIV status is based on self-report. In other words, if the notes say that the "patient reports being positive since 1999," you should select "No."
- If you select "Yes," complete the date field.

IX. Clinical Status

Clinical Record Reviewed

- Select "Yes" to the Clinical Record reviewed question if a medical record abstraction was completed for the case. If you contact a provider and obtain a detailed amount of information over the phone, you should also select "Yes" for clinical record reviewed.
- Select "No" if you are completing the form based on information obtained through a DIS interview, STD*MIS, vital records or any other health information database that does not contain a complete medical record.

Symptomatic Infection

- Enter the date of documented asymptomatic infection.

Asymptomatic Infection

- Enter the date of documented asymptomatic infection.

AIDS Indicator Diseases

- Complete this section with any AIDS indicator diseases. Refer to *Appendix 5: AIDS Indicator Diseases* for a listing of all AIDS Indicator Diseases. For each medical record abstraction, it is important to refer to *Appendix 5: AIDS Indicator Diseases* to ensure that all appropriate AIDS Indicator Diseases are included. Complete the AIDS indicator disease exactly as it is shown in Appendix 5.
- Select "Def" for a definitive diagnosis or "Pres" for a presumptive diagnosis. Definitive diagnoses are based on specific laboratory methods such as histology or culture. Presumptive diagnoses are made by the clinician based on history/observations.
- Enter the date that the indicated disease was initially diagnosed.
- If more than 5 AIDS Indicator Diseases are identified, note the additional diseases in the Comments section, and indicate definitive or presumptive diagnosis and the initial diagnosis date.

RVCT Case Number

- If the case has been diagnosed with *Mycobacterium tuberculosis*, enter the RVCT case number in the last field.

If HIV tests were not done, does this patient have an immunodeficiency that would disqualify him/her from AIDS case definition?

- Select "Yes" if HIV tests were NOT done and the patient has an immunodeficiency that disqualifies him/her from the AIDS case definition. These include but are not limited to:
  - High-dose or long-term systemic corticosteroid therapy or other immunosuppressive/cytotoxic therapy within 3 months before the onset of the AIDS-defining clinical condition.
  - Any of the following diseases diagnosed before or within 3 months after the AIDS-defining clinical condition was diagnosed:
    - Hodgkin's disease
    - non-Hodgkin's lymphoma (other than primary brain lymphoma)
    - lymphocytic leukemia
    - multiple myeloma
    - any other cancer of lymphoreticular or histiocytic tissue
    - angioimmunoblastic lymphadenopathy
    - a genetic (congenital) immunodeficiency syndrome or an acquired immunodeficiency syndrome atypical of HIV infection, such as one involving hypogammaglobulinemia.

XI. Treatment

- Complete the treatment section by selecting the appropriate check boxes.
- Only complete this section if you have documented evidence in the source you are reviewing that indicates the treatment information.

At time of HIV/AIDS diagnosis, medical treatment was primarily reimbursed by:

- Select the appropriate reimbursement method after investigating the case. Refer to the table below for list of reimbursement methods.

Reimbursement Method
CHAMPUS/TRICARE
CHIP
Medicaid
Medicaid, pending
Medicare
Other public funding
Private insurance, HMO
Private insurance, PPO
Private insurance, unspecified
Self insured
State funded, COBRA
State funded, other
State funded, unspecified
VA
No health insurance
Other
Unknown

For Women:

- Complete the For Women section if applicable.

For Child:

- Enter each child separately.
- Enter the child's name, stateno and date of birth.
- Enter the hospital of birth, with the appropriate address information.
- If you identify information on more than 1 child, this information should be completed in the Comments Section by including all information listed above.

XIV. Local Fields

- Please note that Local fields are not transmitted to the CDC.

Prison Facility

- If the person was in prison at the ACRF was completed, enter the name of the correctional facility in the Correctional Facility local field. If a case was moved from one correctional facility to another, both correctional facilities can be indicated here. Separate multiple facilities with a ";"

Partner's Name

- Enter any Partner's Names for the case as Last Name, First Name. If multiple partners are identified, separate with a ";". Please ensure that the order of Partner's Name to Partner's Stateno is retained. If you do not have a Partner's Name but you have a Partner's Stateno, enter N/A in the Partner's Name field.

Partner's Stateno

- Enter any Partner's Stateno's for the case. If you have multiple partner's Stateno's, separate with a ";". Please ensure that the order of Partner's Name to Partner's Stateno is retained. If you do not have a Partner's Stateno but you have a Partner's Name, enter N/A in the Partner's Stateno field.

Previous HIV History

- If you identify previous unreported HIV history, such as diagnoses prior to 1999, enter this information.

Lab Name of First Positive Test

- For all "New Case" reports whose diagnosis occurred in the last 6 months, enter the name of the lab that conducted the confirmatory HIV lab test for this case report form. For example, if the lab conducting the EIA is different from the lab conducting the Western Blot, you should enter the name of the lab conducting the Western Blot. If a case was diagnosed more than 6 months ago please complete the field with "Old Diagnosis" If the laboratory name is not known, complete this field with "UNKNOWN". **This field should be completed for all new cases.**

Earliest Drug Resistance Test

- For all "New Case" reports if you find documentation in the medical record that a HIV drug resistance test was performed, enter the name of the laboratory that conducted the resistance test and the date the test was performed. If there are multiple resistance tests in the medical record enter the lab name and date corresponding to the earliest test. If there is no evidence of a resistance test in the record, complete this field with "No Resistance Test." **This field should be completed for all new cases**.

XV. Testing and Treatment History

General Guidance

- Surveillance sites are required to complete the TTH data elements on the ACRF for all newly reported adult HIV cases.
- This section of the ACRF is the only section where patient self-reported information is acceptable.
- The following are descriptions of the common response options for the TTH data elements:

Response	Description
Yes	Indicates that there was sufficient documented evidence that the event occurred. Evidence can be from patient self-report, health care provider note, or laboratory documentation.
No	Indicates that there was sufficient documented evidence that the event did not occur. Evidence can be from patient self-report or health care provider documentation of no previous negative test.
Unknown	Indicates that the patient reported "don't know", the health care provider documented "unknown", or there was insufficient documented evidence for or against (supporting or denying) the occurrence of the event.
Refused	Indicates patient refused, health care provider recorded "refused", or facility refused to permit the medical record review.

Blank	Indicates that the usual data sources were not investigated and/or the health care provider/staff were not asked.

Main Source of Testing and Treatment History Information

- Select the appropriate box to indicate the source of information for the TTH form. If the source of data is unknown, then leave blank.

Source Type	Description
Provider Report	Information was obtained from a report submitted by a health care provider or from a phone call with a provider. Information was found by the provider from chart notes, laboratory reports, or recollection from discussion with the patient or another health care provider.
Patient Interview	Patient was directly asked these questions by DIS, a counseling and testing provider or someone who has received some training in the proper collection of TTH information
Medical Record Review	Health Department staff obtains the information through review of medical charts or electronic medical record.
Other	Information was obtained from another source.

- Only one box may be checked per form. If information comes from more than one source, then additional ACRF forms, one for each source, should be completed.

Date Patient Reported Information

- Fill in month, day and year completely.
- The variable represents different dates, depending on the circumstances in which the information was primarily obtained.

Source Type	Date Patient Reported Information
Patient Interview	Date of interview
Medical Record Review	The last date of the patient encounter or provider's note that contributed to the TTH information reported in this ACRF. Do not use the actual medical record review date unless there is no other date to use.
Provider Report	The date when most of this information was obtained from the patient or another data source, or, lacking that, the date when the provider completed the report.
Other	The date information was obtained from another source.

- Do not leave this date blank. This date will be used for prioritizing the selection of incidence data in eHARS person view when there are multiple TTH documents. If the date patient reported information is unknown, enter the date when the document was received at the health department.

Ever had a previous positive HIV test?

- This provides information about the patient ever having a positive HIV test before the current test.
- Answer with the response Yes, No, Unknown, or Refused as described in general guidance above.

Date of First Positive HIV test

- This is the date of the earliest known positive HIV test for the patient. This date could be from an anonymous test that will never be reported to the national HIV surveillance system.
- Enter the date (MM/DD/YYYY) of the **first positive** HIV test. If the day is unknown, enter the MM/../YYYY. If the month is unknown, leave the month blank and just enter the year (YYYY).
- For the TTH section of the ACRF, this date is often self-reported.
- Do not report indeterminate or false positive tests.

Ever had a negative HIV test?

- Check whether the patient has ever tested **negative** for HIV. Answer with the response Yes, No, Unknown, or Refused. See general guidance above.
- Self-reported information is acceptable.
- If yes, then enter the date (MM/DD/YYYY) of the **last negative** test. If the day is unknown, enter MM/../YYYY. If the month is unknown, leave the month blank and just enter the year (YYYY).
- If the individual never had a negative HIV test prior to the first positive test mark "No"
- Unknown should only be marked if the patient did not know if s/he has ever tested negative or all potential sources of information were reviewed and there was no information about the patient's negative tests history.
- Last negative refers to a negative confirmatory test.
- If Unknown is marked, **do not** answer the next question "Number of negative HIV tests within 24 months before first positive test"

Number of negative HIV tests within 24 months before first positive test (do not include first positive test)

- The purpose of this variable is to indicate testing frequency in the 24 months before the first positive HIV test in order to calculate the inter-test interval for repeat testers where there is no date of last negative test. Indicate the number of times the patient has tested in the **24 months** before his/her first positive test.
- This question is often misinterpreted. Note that:
    1. Include only tests during the 24 months prior to the first positive test, whenever it was.
    2. By definition, prior tests must be negative because they come before the first positive.

    Examples:
    1. If a patient's first positive test was today and he indicates that he tested negative three other times in the past 24 months, his total will be 3 tests.
    2. If a patient's first positive test was also his first ever test, his total will be 0.
    3. If a patient had five negative tests in his lifetime, but only two were in the 24 months before the first positive then the total would be 2.

Has the patient ever taken any Antiretroviral medications?

- Check whether the patient has taken any antiretroviral (ARV) medications prior to his/her first positive test. This includes highly active-antiretroviral therapy (HAART) or ARV, some medications for hepatitis, and post-exposure prophylaxis for HIV. Self-reported data are acceptable.

- If yes, then list the medications.
- If yes, then indicate the start date (MM/DD/YYYY). If exact date is unknown include the month and year or just year.
- If yes, then indicate the end date (MM/DD/YYYY). If exact date is unknown include the month and year or just year.
- If the patient is currently taking medications and has not completed the regimen check the Currently Taking check box and leave the end date field blank.

XV. Comments

- Include any additional comments on the case in this section. Enter only comments that are pertinent to HIV surveillance.
- Please note that comments are not transmitted to the CDC.

APPENDIX 1: Document Source Codes

A01 Inpatient Record

A01.01	IPR/Acute Care Facility
A01.02	IPR/VA Hospital
A01.03	IPR/Military Hosp
A01.04	IPR/Long Term Care Fac
A01.05	IPR/Hospice

A02 Outpatient Record

A02.01	OPR/HMO
A02.02	OPR/VA Clinic
A02.03	OPR/Private Physician
A02.04	OPR/Adult HIV Clinic
A02.05	OPR/Infect Disease Clinic
A02.06	OPR/County Health Depart Clinic
A02.07	OPR/Maternal HIV Clinic
A02.08	OPR/Prenatal Clinic
A02.09	OPR/Pediatric HIV Clinic
A02.10	OPR/OBGYN
A02.11	OPR/Pediatric Clinic
A02.12	OPR/TB Clinic
A02.14	OPR/Indian Health Service
A02.15	OPR/Early Interv Nurse
A02.16	OPR/Visiting Nurse Service
A02.17	OPR/Hemophilia Trmnt Center
A02.18	OPR/Hospice
A02.19	OPR/Drug Treatment Center
A02.20	OPR/Rehabilitation Center
A02.25	OPR/Other Clinic

A03 ER Record N/Resulting in Admission

A04 Screening,Diagnosis,Referral

A04.01	SDR/Blood Bank
A04.02	SDR/Drug Treatment Clinic
A04.03	SDR/Family Planning Clinic
A04.04	SDR/HIV Case Management Agency
A04.05	SDR/HIV Counseling, Testing Site
A04.06	SDR/Immigration
A04.07	SDR/Insurance Report
A04.08	SDR/Job Corps
A04.09	SDR/Military
A04.10	SDR/Partner Counseling Service
A04.11	SDR/STD Clinic
A04.12	Public Health Notes

A05 Laboratory

A05.01	Laboratory/Hospital
A05.02	Laboratory/State
A05.03	Laboratory/Private

A06 Other Database

A06.01	OD/AIDS Drug Assist Prog ADAP
A06.02	OD/ASD
A06.03	OD/Birth Certificate
A06.04	OD/Birth Defects Registry
A06.05	OD/Cancer Registry
A06.06	OD/Database Provided by Coroner
A06.07	OD/Death Certificate
A06.08	OD/EHRAP
A06.09	OD/EPS
A06.10	OD/HARS
A06.11	OD/Health Department Records
A06.12	OD/Hepatitis Registry
A06.13	OD/Hosp Bill/Discharge Records
A06.14	OD/HRSA HIV Care
A06.15	OD/Immunization Registry
A06.16	OD/Medicaid Records
A06.17	OD/NDI Search
A06.18	OD/Out of State Reports
A06.19	OD/Prison, Jail, Oth Correc Fac
A06.20	OD/PSD
A06.21	OD/State Disease Registry
A06.22	OD/SHAS
A06.23	OD/SHDC
A06.24	OD/STD Registry
A06.25	OD/Tuberculosis Registry
A06.27	OD/Vital Statistic State/Local
A06.28	OD/HARS NDI

A07 Other Facility Record

A07.01	OFR/Prison, Jail, Oth Correc Fac
A07.02	OFR/Coroner
A10.01	COPHI Investigation

APPENDIX 2: State Abbreviations

Abbreviation	State
AK	Alaska
AL	Alabama
AQ	American Samoa
AR	Arkansas
AZ	Arizona
BQ	Navassa Islands
CA	California
CO	Colorado
CQ	Mariana Island
CT	Connecticut
DC	District of Columbia
DE	Delaware
FC	Foreign Country
FL	Florida
FM	Micronesia
GA	Georgia
GQ	Guam
HI	Hawaii
IA	Iowa
ID	Idaho
IL	Illinois
IN	Indiana
JQ	Johnston Atoll
KS	Kansas
KY	Kentucky
LA	Louisiana
MA	Massachusetts
MD	Maryland
ME	Maine
MI	Michigan
MN	Minnesota
MO	Missouri
MQ	Midway Island
MS	Mississippi
MT	Montana
NC	North Carolina
ND	North Dakota
NE	Nebraska
NH	New Hampshire
NJ	New Jersey
NM	New Mexico
NQ	Trust Territories
NV	Nevada
NY	New York
OH	Ohio
OK	Oklahoma
OR	Oregon
PA	Pennsylvania
PR	Puerto Rico
RI	Rhode Island
RM	Marshall Island
RQ	Puerto Rico
SC	South Carolina
SD	South Dakota
TN	Tennessee
TX	Texas
UT	Utah
VA	Virginia
VQ	Virgin Islands
VT	Vermont
WA	Washington
WI	Wisconsin
WQ	Wake Island
WV	West Virginia
WY	Wyoming

APPENDIX 3: Extended Races

Extended Races
Central American
Cuban
Dominican
Mexican
Puerto Rican
South American
Spain/Portugal
Chinese
Filipino
Japanese
Korean
Asian Indian
Vietnamese
Laotian
Thai
Cambodian
Pakistani
Indonesian
Hmong
Burmese
Bangladeshi
Sri Lankan
East Indian
Malayan
Okinawan
Taiwanese
Singaporean
Pacific Islander
Samoan
Tongan
Tahitian
Guamanian
North Mariana
Palauan
Fijian
Micronesian
Alaska Native
Aleut
Eskimo Indian
American Indian
Cajun

APPENDIX 4: Facility Types

Code	Facility Type
F.OTH	(F.OTH) Facility/Other
F.UNK	(F.UNK) Facility/Unknown
F01	(F01) Inpatient Facility [IP Fac]
F01.01	(F01.01) IP Fac/Hospital
F01.04	(F01.04) IP Fac/Long Term Care
F01.50	(F01.50) IP Fac/Drug Treatment
F01.OTH	(F01.OTH) IP Fac/Other
F01.UNK	(F01.UNK) IP Fac/Unknown
F02	(F02) Outpatient Facility [OP Fac]
F02.01	(F02.01) OP Fac/HMO Clinic
F02.03	(F02.03) OP Fac/Prvt Physician's Office
F02.04	(F02.04) OP Fac/Adult HIV Clinic
F02.05	(F02.05) OP Fac/Infectious Disease Clinic
F02.09	(F02.09) OP Fac/Ped HIV Specialty Clinic
F02.10	(F02.10) OP Fac/OBGYN Clinic
F02.11	(F02.11) OP Fac/Pediatric Clinic
F02.12	(F02.12) OP Fac/TB Clinic
F02.16	(F02.16) OP Fac/Home Health Agency
F02.17	(F02.17) OP Fac/Hemophilia Trmnt Center
F02.18	(F02.18) OP Fac/Hospice
F02.19	(F02.19) OP Fac/Drug Treatment Center
F02.25	(F02.25) OP Fac/Other Clinic
F02.50	(F02.50) OP Fac/ACTG Site
F02.51	(F02.51) OP Fac/Community Health Center
F02.52	(F02.52) OP Fac/Employee Health Clinic
F02.53	(F02.53) OP Fac/Hlth Dpt/Pub Hlth Clinic
F02.54	(F02.54) OP Fac/Mobile Clinic
F02.55	(F02.55) OP Fac/Non-mobile Street Outrch
F02.56	(F02.56) OP Fac/PACTG Site
F02.57	(F02.57) OP Fac/Pri Care Clinic, N/Spec
F02.58	(F02.58) OP Fac/School or Univ Clinic
F02.OTH	(F02.OTH) OP Fac/Other
F02.UNK	(F02.UNK) OP Fac/Unknown
F03	(F03) Emergency Room
F04	(F04) Screening/Diagnostic/Referral [SDR]
F04.01	(F04.01) SDR/Blood Bank/Plasma Center
F04.02	(F04.02) SDR/Drug Treatment Center
F04.03	(F04.03) SDR/Family Planning Clinic
F04.04	(F04.04) SDR/HIV Case Mgmt Agency
F04.05	(F04.05) SDR/HIV Counseling, Testing Site
F04.07	(F04.07) SDR/Insurance Screening
F04.11	(F04.11) SDR/STD Clinic
F04.OTH	(F04.OTH) SDR/Other
F04.UNK	(F04.UNK) SDR/Unknown
F05	(F05) Laboratory
F07	(F07) Other Specific Facility [OS Fac]
F07.01	(F07.01) OS Fac/Correctional Facility
F07.02	(F07.02) OS Fac/Coroner or Med Examiner

APPENDIX 5: AIDS Indicator Diseases

AIDS INDICATOR DISEASES
Candidiasis, bronchi, trachea, or lungs
Candidiasis (esophageal)
Carcinoma (invasive cervical)
Coccidioidomycosis (disseminated or extra-pulmonary)
Cryptococcosis (extra-pulmonary)
Cryptosporidiosis, Chronic Intestinal >1 month duration
Cytomegalovirus Disease (other than in liver, spleen, or nodes)
Cytomegalovirus Retinitis (with loss of vision)
HIV Encephalopathy
Herpes Simplex: chronic ulcers >1 month duration or bronchitis, pneumonitis, or esophagitis
Histoplasmosis (disseminated or extra-pulmonary)
Isosporiasis - chronic intestinal >1 month duration
Kaposi's Sarcoma
Lymphoma Burkitt's (or equivalent term)
Lymphoma Immunoblastic (or equivalent term)
Lymphoma, primary in brain
Mycobacterium avium complex or M kansasii, (disseminated or extra-pulmonary)
M tuberculosis, pulmonary
M tuberculosis, (disseminated or extra-pulmonary)
Mycobacterium of other species or unidentified species, (disseminated or extra-pulmonary)
Pneumocystis carini pneumonia
Pneumonia, recurrent, 12 month period
Progressive mulitfocal leukopencephalopathy
Salmonella septicemia, recurrent
Toxoplasmosis of the brain
Wasting syndrome due to HIV

Appendix G

(PCRF not included. Please contact your local HIV Surveillance program to request information about the case report form)

Instructions for Completing the PCRF

Report status

- Check the appropriate status of the report. This a required field on all documents.

Report Status	Description
New Case	A PCRF for a case that has never been reported in eHARS. A new case can be a newly reported perinatal exposure, perinatal seroreverter, HIV (non-AIDS) or a concurrent diagnosis for HIV and AIDS.
Update to HIV	A PCRF for an HIV diagnosis of a case that has been reported to eHARS as a perinatal exposure.
Update to AIDS	A PCRF for an AIDS diagnosis of a case that has been reported to eHARS with only an HIV diagnosis.
Other Update	A PCRF containing updated information on an existing case in eHARS.

TDCJ Case

- Check the box for cases known to be in a TDCJ facility at the time of PCRF completion.

Stateno

- If the PCRF is for a "New Case", assign a unique stateno.
- If the PCRF is for an "Update to HIV", "Update to AIDS" or "Other Update", fill in the eHARS stateno which has already been assigned.
  - **NOTE**: The eHARS stateno should be used for ALL "Update to AIDS" cases – even if the case is progressing from HIV to AIDS in a different jurisdiction. "Update to AIDS" cases will not be assigned a new stateno, even if the case was diagnosed with AIDS in a different jurisdiction.

I. Form Information

- All information in the form section of the PCRF must be filled out to be considered a complete report.

Document Source

- The source from which the information on the PCRF was gathered.
  - A PCRF can only have **one** document source. If you attain information on a case from multiple sources, then you must complete a separate PCRF for each of the sources.
  - Only the information gathered from a particular document source should be used to complete the PCRF (i.e., a PCRF should not contain information from more than one source).

- Use the document source codes provided by the CDC to complete this field. The most common document source codes are listed below. A full list of document source codes can be found in *Appendix 1: Document Source Codes*.
  - If you are unsure which document code to use, please contact Central Office for guidance.

Most common sources:

Source Code	Description
A01.01	Inpatient Hospital
A01.02	Inpatient VA
A02.02	Outpatient VA
A02.03	Outpatient Private Physician
A02.04	Outpatient Adult HIV Clinic
A02.05	Outpatient Infect Disease Clinic
A02.06	Outpatient County Health Depart Clinic
A02.07	Outpatient Maternal HIV Clinic
A02.08	Outpatient Prenatal Clinic
A02.09	Outpatient Pediatric HIV Clinic
A02.10	Outpatient OBGYN
A02.25	Outpatient Hospital
A04.01	Blood Bank (Plasma Center)
A04.05	HIV Counseling, Testing Site
A04.11	STD Clinic
A04.12	DIS Notes (reviewed actual notes)
A06.24	STD*MIS (looked case up in database)
A07.01	Prison, Jail, Other Correctional Facility

Report Medium

- The medium through which you learned about the case. See the table below for selecting the appropriate report medium.

Report Medium	Description
Field visit	Medical record abstraction performed at the facility
Mail	Facility directly mailed information
Phone	Spoke to facility over the telephone to gather information
Electronic Transfer	Information transferred electronically (e.g. RIDR or info on an FTP site)
Disk-CD	Information transferred to site via portables media (e.g. cd)

- If STD*MIS is the source of the information on the PCRF, select “paper form, field visit” as the report medium

Surveillance Method

- The method through which you learned about the case.
- Selecting the appropriate surveillance method is extremely important because this variable is used in the national evaluation plan. See the table below for a description of each of the surveillance methods.

Surveillance Method	Description/Example
Active	You INITIATE a process to obtain a report or gather information. For example, you go to a facility and ask for a list of all of their HIV patients, and in doing this, you learn of a new case.
Passive	You receive a report WITHOUT specifically requesting it. For example, a facility calls you to report a new case. Note that this information must be unsolicited (i.e. you did not call the facility about the case first)
Follow-up	You actively gain information because of a prior report. For example, you call a facility in order to gain more information on a case that you received a lab document for.
Re-abstraction	Not to be used at this time
Unknown	You should always know how you learned about a case, so only under rare circumstances should you select unknown

Note that the surveillance method for most cases will be "Follow-up," because surveillance staff generally learn about most cases through lab reports or the annual birth certificate match; thus, the completion of the PCRF is a follow-up to the lab report or birth certificate match

Date Form Completed

- Enter the date on which you completed the PCRF.

Person Completing Form

- Enter the name of the person completing this PCRF.
  - For surveillance staff, enter your three letter initials only (e.g. MRF). If surveillance staff do not have a middle initial, enter the first and last initial, separated by an underscore (e.g. M_F).
  - For staff who are not surveillance staff (e.g. staff at a clinic), enter your entire name (Last Name, First Name) including your credentials (e.g. MD).

Facility where Information was obtained

- Enter the name of the facility from which the information was gathered, including the corresponding facility type.
  - You must use the exact facility name listed on the excel spreadsheet, which was provided to you by Central Office
  - Please refer to the facility of diagnosis section (VII. Facility of Diagnosis) below for specific instructions on completing facility name fields, including facility type and facility setting, using the list provided by the Central Office.
- If you gathered the information from STD*MIS, refer to your facility list to identify the correct facility name to enter in this field

II. Name

Name Type

- Select the appropriate name type for each name completed and complete the full name of the case. See the list below for available name types.

- For a "New Report", the legal name must be on the form.

Name Type	Description
Legal	Person's legal name
Alias	Person's assumed name
Maiden	Person's name immediately before a first marriage; in most cases, equal to birth name
Married	Name assumed from a partner in a marital relationship
Nickname (Call me)	Person's preferred name when directly addressed, such as a nickname or street name
Birth	Person's name at birth
License	Person's name when granted a license to practice a profession or when issued a formal certificate
Display	The name displayed in a system (for example, a hospital's medical records system) as the primary name for a patient
Indian/Tribal	Person's Indian, indigenous, or tribal name
Professional	Person's professional name, such as a pseudonym or pen name, or an abbreviation of a professional organization or title entered in the Suffix field
Religious	Person's religious name instead of a secular name
Record	Person's officially written and preserved name on record, such as in judicial proceedings

Name

- Include all available name parts (first, middle, last, prefix, and suffix). Spell the name exactly as it appears in the document source, including any punctuation like dashes (-) or apostrophes ('').
- If there are more than two names in one document source, list the additional names and their corresponding name type in the Comments section.

III. Current Address

Address Type

- Select the appropriate address type for the most current address listed in the document source being reviewed. Below is a list of address types available in eHARS.

Address Type	Description
Residential	Address of a residence
Correctional	Address of a correctional facility (including jails)
Homeless	Address of a location where a homeless person spends most of their time. Homeless should only be used with documented evidence that the patient is homeless and not because an address could not be found.
Foster home	Address of a foster home
Bad address	Address is known to be for a place that does not exist.
Postal	A PO box address or the address of a mail receipt facility
Residence at death	Person's residence at time of death

Residence at birth	Person's residence at time of birth
Shelter	Address of a shelter
Temporary	Address of a short term (temporary) residence

Address

- Enter the patient's most current address listed in the document source being reviewed. Be sure to enter the patient's complete address, including street address and zip code.
- If the patient is homeless, record the zip code for the where the person spends most of their time. If this information is not available then enter the zip code for where the person was tested.
- Since eHARS can accommodate more than one address, if a patient has a temporary address or is only temporarily residing in a shelter or correctional facility you should also record the patient's residential address if available. Additional addresses should be recorded in the Comments section, including the address type.

IV. IDs

- List all patient IDs and corresponding ID type. List any additional IDs in the comments section, including the type of ID.

ID Type

- Select the appropriate ID type. Below is a list of ID types available in eHARS.

ID Type
Medical Record Number
OOS Stateno
Prison Number
RVCT (TB) Number
Social Security Number (SSN)
Social Security Number Alias
STD*MIS Number

- For OOS (out of state) cases, include the two letter abbreviation of the other state in the ID type field "other." Use the format <two letter state abbreviation> stateno (e.g. "LA stateno").

ID

- Enter the full ID for each ID type selected.

V. Demographic Information

Diagnostic status

- Select the diagnostic status of the case. Refer to Chapter 5-Appendix A for the 2008 revised surveillance case definition for HIV infection regarding the appropriate diagnostic status to record for this question.

Date of Last Medical Evaluation

- Enter the date the patient was last medically evaluated, regardless of reason for exam. This includes emergency room visits.

Date of Birth / Alias Date of Birth

- Enter the patient's date of birth as it appears in the document source. If the date of birth is known to be an alias date of birth, then complete the alias date of birth field with this date of birth.

Vital Status/Date of Death/St of Death

- Check the appropriate vital status box. If the case is deceased, the date of death and state of death fields must be completed. Use the state's two letter abbreviation. Use the code "FC" (foreign country) for cases whose place of death is outside of the United States. Refer to *Appendix 2: State Abbreviations* for a list of the two letter state codes.

Date of Initial Evaluation for HIV Infection

- Enter the date of initial evaluation for HIV infection.

Sex at Birth

- Select the sex of the patient at birth. If the patient's current sex is different than their sex at birth, note this in the Comments section.

Ethnicity

- Check the appropriate box. If ethnicity cannot be found, then select "Unknown."

Race

- Check the appropriate box or boxes. If race cannot be found, then select "Unknown."

Extended Race

- If you know the extended race of a case then complete this field using one of the extended races listed in *Appendix 3: Extended Races*.

Country of Birth

- Check the appropriate box. For cases not born in the USA, write in the full name of the country of birth.

VI. Residence at Exposure and Diagnosis

Perinatal Exposure Residence

- Complete the perinatal exposure residence section if the PCRF is for a new perinatal exposure.
- The perinatal exposure residence is the residence of the parent/guardian of the child at the time of exposure.
- Select the "Same as current address" box if the patient's residence at perinatal exposure is EXACTLY the same (including street address) as their current residence (Section III.). If the perinatal exposure residence is not exactly the same as the current address complete all fields in this section. Do not select "Same as current address" if current address is not listed on the PCRF.

Seroreverter Residence

- Complete the seroreverter residence section if the PCRF is for a seroreverter diagnosis.
- The seroreverter residence is the residence of the parent/guardian of the child at the time of seroreverter diagnosis.
- Select the "Same as current address" box if the patient's residence at seroreverter diagnosis is EXACTLY the same (including street address) as their current residence (Section III.). If the seroreverter residence is not exactly the same as the current address complete all fields in this section. Do not select "Same as current address" if current address is not listed on the PCRF.

HIV Residence

- Complete the HIV residence section if the PCRF is for an HIV diagnosis (including concurrent* HIV and AIDS diagnoses).

---

* Concurrent Diagnosis is defined as AIDS diagnosis within one calendar month of HIV diagnosis

- The HIV residence address is the residence where the patient was living at the time of HIV diagnosis.
- Select the "Same as current address" box if the patient's residence at HIV diagnosis is EXACTLY the same (including street address) as their current residence (Section III.). If the HIV diagnosis residence is not exactly the same as the current address complete all fields in this section. Do not select "Same as current address" if current address is not listed on the PCRF.

AIDS Residence

- Complete the AIDS residence section if the PCRF is for a new AIDS diagnosis (including concurrent* HIV and AIDS diagnoses).
- The AIDS residence address should be the residence that the patient was living at the time of AIDS diagnosis.
- Select the "same as current address" box if the patient's residence at diagnosis is EXACTLY the same (including street address) as their current residence (Section III.). Do not select "Same as current address" if current address is not listed on the PCRF.

VII. Facility of Exposure

- Complete the perinatal exposure fields for new perinatal exposure reports.
- The facility of perinatal exposure is the facility where the child received the initial evaluation for HIV infection.
- Complete the perinatal exposure facility of diagnosis fields using the list supplied by the Central Office. You must use the exact facility name and corresponding facility type listed on the excel spreadsheet. This list will periodically be updated and distributed to HIV/AIDS surveillance staff at the local and regional health departments.
- The list consists of the facility's ID number as it is stored in eHARS, facility name, city, state, and facility type. The spreadsheet is organized by HIV/AIDS reporting site; to navigate to the different sites, click on the arrows located at the lower left hand corner of the spreadsheet.
    - Because facilities may have more than one Facility Type assigned, be certain to select the facility name with the correctly associated facility type from the search results. For example, JPS HOSP has more than one facility type associated with it, including Inpatient Facility/Hospital, Outpatient Facility/Hospital, and Emergency Room. Please refer to the facility type list located in *Appendix 4: Facility Types* for the complete list of facility types.
    - If the combination of the facility name, city, state and type cannot be found on the list, indicate that the facility needs to be added to the list by checking the 'New Facility' box. **NOTE**: If you come across a facility on the list that is not listed with the facility type you are looking for, then indicate that it is a new facility.
- For out-of-state facilities, complete the facility of diagnosis field with OOS and the two letter abbreviation for the state. For example, if the facility of diagnosis is in Louisiana, then the write "OOS LA" in the facility of diagnosis field. Complete the State field and leave the remaining address fields blank, including City. For Facility Type, write 'Unknown' in the Other field.
  Similarly, for foreign country facilities, complete the facility of diagnosis field with OOC and the two letter abbreviation for the country. Country abbreviations can be found at this website: http://www.worldatlas.com/aatlas/ctycodes.htm
  Leave the address fields blank and write 'Unknown' in the Other field under Facility Type.
- For insurance companies, refer to the facilities list to identify whether this insurance company has been added to eHARS. If this insurance company is new to the facility

list, check "New Facility", complete the name of the insurance company and write "INSURANCE SCREENING" in the Other field under Facility Type.

- For Private Physicians, Central Office will no longer use PVT PHYS and the regional designation. Physician names will be entered in the following format: PVT-LName, FName Credential. For example, Dr. Joe Smith MD, would be entered as follows: PVT-Smith, Joe MD
  Complete the city and state information, and select Private Phys for the type.

VIII. Facility of Seroreverter Diagnosis or HIV/AIDS Diagnosis

- If the child is classified as a seroreverter, check "Facility of Seroreverter Diagnosis" and complete the corresponding facility fields. Note: The facility of seroreverter diagnosis is the facility where the child received the last evaluation for HIV infection necessary to classify the child as a seroreverter.
- If the child is classified as HIV infected, check "Facility of HIV Diagnosis" and complete the corresponding facility fields. Note: The facility of HIV diagnosis is the facility where the child received the evaluation for HIV infection necessary to classify this person as HIV infected. Refer to Chapter 5-Appendix A for information regarding the child's HIV diagnosis.
- For new AIDS diagnosis reports, complete the AIDS Diagnosis fields.
- Complete the seroreverter, HIV and AIDS facility of diagnosis fields using the list supplied by the Central Office. You must use the exact facility name and corresponding facility type listed on the excel spreadsheet. This list will periodically be updated and distributed to HIV/AIDS surveillance staff at the local and regional health departments.
- Refer to Section VII for further information regarding facility completion.

IX. Personal History (Maternal)

Child's biological mother's infection status

- Check the appropriate response depending on the mother's timing of HIV diagnosis based on her first positive HIV test as it relates to the child's date of birth. (Verify the mother's date of HIV diagnosis as documented in eHARS, resolve any discrepancies, and complete an updated ACRF if necessary.)

Date of mother's first positive HIV confirmatory test

- Complete the date of the mother's first positive HIV confirmatory test.

Mother was counseled about HIV testing during the pregnancy, labor or delivery

- Select "Yes", "No" or "Unknown". Select "Yes" if the mother was counseled anytime during pregnancy or labor and delivery regarding the risks of HIV in pregnancy, benefits and meaning of HIV testing.

Biologic mother had heterosexual relations with any of the following

- Information on risk factors should be collected for risk factors occurring prior to the first positive HIV test or AIDS diagnosis for the mother. (Risk factor information on the mother refers to behaviors that started before the child's birth.)
- Complete all subsequent questions of the maternal personal history section by selecting "Yes", "No" or "Unknown".
- Select "Yes" if you find documented evidence in that document source that the person has that risk factor.
- Select "Unknown" if the personal history is truly unknown after reviewing all of the information in the document source.

- Only select “No” if you find documented evidence that the person does not have the risk factor (e.g. the medical record states “patient has never injected drugs”).
- If you select received clotting factor, complete the clotting factor type and date received.
- If the mother’s personal history on the PCRF differs from eHARS, you must complete an updated ACRF for the mother.
- This section should only be completed if the biologic mother has had documented heterosexual contact. For female cases, the women must have had sex with a male (verify documentation in eHARS).
- Only select “Yes” to the last two options in the Personal History section if this risk factor might be the primary mode of HIV exposure for this case. In other words, you should select “Yes” to these two questions, if the case is believed to have acquired HIV through one of these risk factors. For example, if a case reports that they report that they had a blood transfusion, but they are a known MSM then you would not respond to the transfusion question. Selecting one of these risk factors will initiate a COPHI investigation.
- Do not select “Yes” to the blood transfusion or transplant questions if the transfusion or transplant occurred outside the United States.

X. Personal History (Child)

- Information on the child refers to circumstances or behaviors that exposed the child to HIV. (If the child received a blood transfusion or other treatment after the documentation of HIV infection, do not enter this information on the PCRF.)
- Complete all questions of the child’s personal history section by selecting “Yes”, “No” or “Unknown”.
- Select “Yes” if you find documented evidence in that document source that the person has that risk factor.
- Select “Unknown” if the personal history is truly unknown after reviewing all of the information in the document source.
- Only select “No” if you find documented evidence that the person does not have the risk factor (e.g. the medical record states “patient has never injected drugs”).
- If you select received clotting factor, complete the clotting factor type and date received.
- Only select “Yes” to (“Injected non-prescription drugs”, “Received transplant or tissue/organs”, “Sexual contact with a male”, “Sexual contact with a female”, or “Other documented risk”) in the Personal History section if this risk factor might be the primary mode of HIV exposure for this case. In other words, you should select “Yes” to these five questions, if the case is believed to have acquired HIV through one of these risk factors. Selecting one of these risk factors will initiate a COPHI investigation.
- If other documented Risk is selected, write in the risk factor.

XI. Lab Tests

- All tests marked in this section should be tests that are documented by the source from which you are gathering the information.
  - You should never complete the lab information section using self-reported information
- If you are unfamiliar with a particular test, please refer to Chapter 5 of the manual or call Central Office for further guidance.
- Document additional tests in the comments section.

- For children, in addition to positive tests, document all negative viral detection and antibody tests.

1. HIV Antibody Tests at Diagnosis

- This section should be completed with only antibody tests done at the time of HIV diagnosis. In other words, if a person had two Western Blots you should only record the Western Blot that was performed at the time of HIV diagnosis.
- Be sure to correctly select whether an HIV Antibody is an HIV-1, HIV-2, or HIV 1/2.

2. HIV Detection Tests

- For this section, you should document all detection tests performed on the patient.
- Note that the *HIV-1 RNA PCR (Qual)* test is a qualitative PCR test (i.e. there is not a numeric result for this test only positive or negative). The RNA PCR test for which there is a numeric result (including results with a "<" or ">" result) is a viral load and should be recorded in section 4. Viral Load tests. Document additional HIV detection tests under "Other" writing the exact name of the test on the line provided.
- A **NAAT test** is a qualitative detection test that can be used as a confirmatory test for HIV and so the results from this test should be recorded in this section. Record the results for this test in this section under *HIV-1 RNA PCR (QUAL)*.

3. Immunologic Lab Tests

- For this section you need to record both the first CD4 count/percent performed on the patient and the most recent CD4. If the most recent and the first are same test then record both in the appropriate sections.
- If there are any additional CD4 counts/percents, record these in the comments section of the PCRF.

4. Viral Load Tests

- For this section you need to record all (undetectable, above the limit of detection, and within the limit of detection) viral load results. Because only one viral load test can be entered for each PCRF, record any additional viral load tests or non-detectable viral loads in the Comments section of the PCRF.
- Be sure to select the correct type of viral load test when recording the results and be sure to designate if the viral load is below the limit of detection "BL" (i.e. undetectable), within the limit of detection "WL" or above the limit of detection "AL". If you need help selecting the correct test please refer to Chapter 5 of the manual or contact Central Office for guidance.

5. If HIV tests were not positive or were not done, or the patient is less than 18 months of age, does this patient have an immunodeficiency that would disqualify him/her from the AIDS case definition?

- Select "Yes" if HIV tests were NOT done and the patient has an immunodeficiency that disqualifies him/her from the AIDS case definition. These include but are not limited to:
  - High-dose or long-term systemic corticosteroid therapy or other immunosuppressive/cytotoxic therapy within 3 months before the onset of the AIDS-defining clinical condition.
  - Any of the following diseases diagnosed before or within 3 months after the AIDS-defining clinical condition was diagnosed:
    - Hodgkin's disease
    - non-Hodgkin's lymphoma (other than primary brain lymphoma)
    - lymphocytic leukemia
    - multiple myeloma
    - any other cancer of lymphoreticular or histiocytic tissue
    - angioimmunoblastic lymphadenopathy

- a genetic (congenital) immunodeficiency syndrome or an acquired immunodeficiency syndrome atypical of HIV infection, such as one involving hypogammaglobulinemia.

6. If laboratory tests were not documented, is patient confirmed by a physician as:

- If there are no laboratory tests documented in the source, then you must select "Yes", "No" or "Unk" under "HIV Infected" or "Not HIV Infected" in response to whether or not an HIV diagnosis was documented by a physician.
- In selecting the appropriate response the doctor should explicitly state that the patient is HIV Infected or Not HIV Infected. You should not select "Yes" for "HIV Infected" or "Yes" for "Not HIV Infected" if the person's HIV status is based on self-report or parent/guardian history. In other words, if the notes say the "patient reports being positive since 1999," you should select "No" for "HIV Infected".
- If you select "Yes," complete the date field.

XII. Clinical Status

AIDS Indicator Diseases

- Complete this section with any AIDS indicator diseases. Refer to *Appendix 5: AIDS Indicator Diseases* for a listing of all AIDS Indicator Diseases. For each medical record abstraction, it is important to refer to *Appendix 5: AIDS Indicator Diseases* to ensure that all appropriate AIDS Indicator Diseases are included. Complete the AIDS indicator disease exactly as it is shown in Appendix 5.
- Select "Def" for a definitive diagnosis or "Pres" for a presumptive diagnosis. Definitive diagnoses are based on specific laboratory methods such as histology or culture. Presumptive diagnoses are made by the clinician based on history/observations.
- Enter the date that the indicated disease was initially diagnosed.
- If more than 3 AIDS Indicator Diseases are identified, note the additional diseases in the Comments section, and indicate definitive or presumptive diagnosis and the initial diagnosis date.

M. Tuberculosis (pulmonary)

- Diagnosis: Enter the diagnosis as "Definitive", "Presumptive" or "Unknown". A definite diagnosis is based on laboratory methods such as histology or culture. A presumptive diagnosis is made by the clinician based on history or observation.
- RVCT Case Number/Date of Diagnosis: If the case has been diagnosed with *Mycobacterium tuberculosis (definite or presumptive)*, enter the RVCT case number and the date of diagnosis.

XIII. Birth History

Birth history was available for this child

- If any birth history information is available for section XIII, answer "Yes", otherwise answer "No" or "Unknown". If no birth history is available proceed to section XIV.

Residence at birth

- Enter the patient's residence address based on the mother's residence at time of infant's birth.
- Be sure to enter the patient's complete address, including street address and zip code.
- If the patient is homeless, record the zip code for the where the person spends most of their time. If this information is not available then enter the zip code for where the person was tested.

- For resident addresses outside of this country use the two letter country abbreviations found at this website: http://www.worldatlas.com/aatlas/ctycodes.htm

Birth Hospital

- Enter the name of the facility of birth, including the corresponding facility type.
  - If the child was born at home, enter "Home Birth" and the corresponding city/state/country. If the child is born outside of the country enter "OOC" and the corresponding country name. For out-of-state birth facilities, complete the facility of birth field with OOS and the two letter abbreviation for the state. For example, if the facility of birth is in Louisiana, then the write "OOS LA" in the facility of birth field. Complete the State field and leave the remaining address fields blank, including City. For Facility Type, write 'Unknown' in the Other field. Similarly, for foreign country birth facilities, complete the facility of birth field with OOC and the two letter abbreviation for the country. Country abbreviations can be found at this website: http://www.worldatlas.com/aatlas/ctycodes.htm Leave the address fields blank and write 'Unknown' in the Other field under Facility Type.
  - You must use the exact facility name listed on the excel spreadsheet, which was provided to you by Central Office
  - Please refer to Section VII for specific instructions on completing facility name fields, including facility type and facility setting, using the list provided by the Central Office.

If you gathered the information from STD*MIS, refer to your facility list to identify the correct facility name to enter in this field

Birth Weight

- Enter the birth weight in pounds or grams.

Type of Birth

- Select the appropriate response.

Type of Delivery

- Select the appropriate response.
- If labor and delivery records or birth records are not available use notes from the child's record.

Birth Defects

- Select "Yes", "No", or "Unknown".
- If "Yes", specify the type of birth defect.
- If the ICD-9 code is available in the child's medical record you may use this code otherwise use one of the 6 digit codes (based on the 3 or 5 digit ICD-9 codes) as documented in the child's medical record.

Neonatal Status

- Select the appropriate response and enter the child's gestational age under "Birth Weeks".
- "Full term" is defined as gestational age greater than or equal to 37 weeks and "premature" is defined as gestational age less than 37 weeks.

Prenatal Care

Month of pregnancy prenatal care began

- Record the month of pregnancy the mother began her prenatal care. Select from "01" to "09". For example if prenatal care began during the third month of pregnancy, enter 03. (Round to the next whole month when a fraction of a month is reported.)
- Enter "00" if mother received no prenatal care and enter "99" if the month of first prenatal care visit is unknown.

Total number of prenatal care visits

- Record the total number of prenatal care visits. Do no include visits unrelated to prenatal care in this count.
- If the mother received no prenatal care enter "00" for the number of visits and enter "99" if the mother received prenatal care but the number of visits is unknown.

Did mother receive zidovudine (ZDV, AZT) during pregnancy

- For purposes of data recording, labor and delivery is not considered to be part of the pregnancy.
- Select the appropriate response depending on information available in the medical record. In the absence of evidence of the patient having taken zidovudine, select "No". (Please note that refusal must be clearly documented in the record.)
- If the mother did not receive any antiretroviral therapy during pregnancy, please answer question 5 on page 5 under section XV. Local Fields.

If yes, week zidovudine (ZDV, AZT) started:

- If "Yes" to previous question, enter the week in pregnancy ZDV/AZT was initiated. For example if ZDV was administered beginning the ninth week of pregnancy, enter 09. Enter "99" if mother received zidovudine during pregnancy but week of initiation is unknown.
- If "No" to previous question, enter "00" for the week ZDV/AZT was initiated.
- If ""Unknown" to previous question, enter "99" for the week ZDV/AZT was initiated.

Did mother receive zidovudine (ZDV, AZT) during labor/delivery

- For purposes of data recording, labor and delivery is not considered to be part of the pregnancy.
- Select the appropriate response depending on information available in the medical record. In the absence of evidence of the patient having taken zidovudine, select "No". (Please note that refusal must be clearly documented in the record.)
- If mother did not receive any antiretroviral therapy during labor and delivery, please answer question 6 on page 5 under section XV. Local Fields.

Did mother receive zidovudine (ZDV, AZT) prior to this pregnancy

- Select the appropriate response.

Other Antiretroviral (ARV) Therapy

- Select the appropriate response. If mother received other antiretroviral therapy during pregnancy or at labor and delivery then record the medication received in the line provided.
- A Single drug formulation often has multiple names. For a complete listing of medications refer to www.aidsinfo.nih.gov. Below is a guide of some of the more common drug formulations.
- If the mother did not receive any antiretroviral therapy during pregnancy, please answer question 5 on page 5 under section XV. Local Fields.
- If the mother did not receive any antiretroviral therapy during labor and delivery, please answer question 6 on page 5 under section XV. Local Fields.

Drug Class	Drug Names
Multi-Class Combinations	Atripla (Efavirenz/Tenofovir/FTC)
Nucleoside/Nucleotide Reverse Transcriptase Inhibitors (NRTIs)	Combivir (AZT/3TC) Emtriva (Emtricitabine, FTC) Epivir (3TC, Lamivudine) Epzicom (Abacavir/3TC, Kivexa) Hivid (Zalcitabine, ddC) Retrovir (Zidovudine, AZT) Trizivir (AZT/3TC/Abacavir) Truvada (Tenofovir/FTC) Videx (Didanosine, ddI) Viread (Tenofovir) Zerit (Stavudine, d4T) Ziagen (Abacavir)
Non-Nucleoside Reverse Transcriptase Inhibitors (NNRTIs)	Intelence (Etravirine, TMC125) Rescriptor (Delavirdine) Sustiva (Efavirenz, Stocrin) Viramune (Nevirapine)
Protease Inhibitors (PIs)	Aptivus (Tipranavir) Crixivan (Indinavir) Invirase (Saquinavir) Kaletra (Lopinavir/Ritonavir) Lexiva (Fosamprenavir, Telzir) Norvir (Ritonavir) Prezista (Darunavir, TMC114) Reyataz (Atazanavir) Viracept (Nelfinavir)
Entry Inhibitors	Fuzeon (Enfuvirtide, T-20) Selzentry (Maraviroc, Celsentri)
Integrase Inhibitors	Isentress (Raltegravir, MK-0518)

Maternal Date of Birth/Soundex/Stateno/Country of Birth

- Record the mother's date of birth, soundex, stateno, and country of birth. Refer to the medical record for the mother's date of birth and country of birth. Refer to eHARS for the mother's soundex and stateno. If necessary complete an update ACRF or complete a new ACRF for this infant's mother.

XIV. Treatment

- Complete the treatment section by selecting the appropriate check boxes.
- Only complete this section if you have documented evidence in the source you are reviewing that indicates the treatment information.

Neonatal zidovudine (ZDV, AZT) for HIV prevention

- Record if the child received any neonatal zidovudine to prevent perinatal HIV infection. Neonatal refers to the time period beginning at birth up to the first six weeks of life.
- Select "Yes", "No", or "Unknown" depending on child's receipt of neonatal zidovudine.
- If "Yes" enter the day, month, and year the child was started on AZT or ZDV as prophylaxis during the first 6 weeks of life.
- If the infant did not receive any antiretroviral therapy, please answer question 7 on page 5 under section XV. Local Fields.

Other antiretroviral therapy (ZDV, AZT) for HIV prevention

- Record if the child received any other neonatal antiretroviral therapy to prevent perinatal HIV infection. Neonatal refers to the time period beginning at birth up to the first six weeks of life.
- Select "Yes", "No", or "Unknown" depending on child's receipt of neonatal antiretroviral therapy.
- If "Yes" enter the day, month, and year the child was started on antiretroviral therapy as prophylaxis during the first 6 weeks of life.
- Refer to the most recent "Guidelines for the Use of Antiretroviral Agents in Pediatric HIV Infection" available at www.aidsinfo.nih.gov for information on antiretroviral therapies.

PCP prophylaxis

- Select "Yes", "No", or "Unknown" depending on child's receipt of PCP prophylaxis.
- If "Yes", enter the day, month, and year the child was started on PCP prophylaxis.
- Examples of PCP prophylaxis include Trimethoprim/sulfamethoxazole (TMP/SMX, Bactrin, Septra), Pentamidine and Dapsone. (TMP/SMX can be used to treat infections other than HIV such as otitis media but is usually used for a shorter period and in this case would not be recorded as "Yes" for this field.)

Was child breastfed

- Select the appropriate response.
- Avoidance of breast-feeding to prevent postpartum transmission of HIV has been recommended for HIV-infected mothers in the United States.
- If there is a suspicion that the child's only exposure to HIV was through breast milk, the local/state NIR coordinator should be alerted.

The child has been enrolled at

Clinical Trial

- Select the appropriate response according to whether the child is enrolled in a clinical trial, particularly if the trial is sponsored by the National Institutes of Health (NIH). Children treated under the AIDS Clinical Trials Group (ACTG) protocols or enrolled in the Women and Infants Transmission Study (WITS) are participating in NIH-sponsored clinical trials.

Clinic

- Select the appropriate response according to whether the child is enrolled in a clinic, particularly if the clinic is sponsored by the Health Resources and Services Administration (HRSA).

At time of perinatal exposure/HIV/AIDS diagnosis, medical treatment was primarily reimbursed by:

- Select the appropriate reimbursement method after investigating the case. Refer to the table below for list of reimbursement methods.

Reimbursement Method
CHAMPUS/TRICARE
CHIP
Medicaid
Medicaid, pending
Medicare
Other public funding
Private insurance, HMO
Private insurance, PPO
Private insurance, unspecified
Self insured
State funded, COBRA
State funded, other
State funded, unspecified
VA
No health insurance
Other
Unknown

The child's primary caretaker is:

- Select the appropriate response based on the person who gives the majority of care for the child.
- For children living with one or two biological parents select "biological parent(s)".
- "Other relative" refers to children living with an aunt, grandmother, etc. in an informal arrangement, and the relative does not receive a stipend for providing care.
- If a child lives with a relative and that relative is paid a stipend for caring for the child, "Foster/Adoptive parent, relative" should be selected.
- A child is considered to be in "foster/adoptive parent, unrelated" care if living with someone other than a relative.
- "Adoptive parent, relative" refers to a child who has been legally adopted by a relative. This includes children with dead parents whose legal custody has been transferred to a relative.
- If the adoptive parent is unrelated please select "foster/adoptive parent, unrelated." This includes children with dead parents whose legal custody has been transferred to a person who is unrelated to the child.
- Social service agency refers to children whose primary caretaker is a social service agency which usually refers to children living in group home situations.
- For children being cared for in situations not described above, select "other" and specify child's primary caretaker, otherwise check unknown.

XV. Local Fields

- Please note that Local fields are not transmitted to the CDC.

Previous HIV History

- If you identify previous unreported HIV history, such as diagnoses prior to 1999, enter this information.

Mother's Last and First Name

- Enter the mother's complete last and first name if available from the medical record. Mother's name should be completed in the last, first format. If the mother is an out of state case please enter "OOS" or "OOC" followed by the two letter abbreviation for the state or the country name immediately after the mother's name. Enter in the following format (enclosing OOS/OOC in parenthesis): Jane Smith (OOS-LA)

Twin's Last and First Name

- Enter the twin's last and first name in the space provided. Complete the Twin's name in the last, first format. For additional siblings born during the current pregnancy, record in the comments section.

Child's Follow-up Status

- Mark the appropriate response depending on the child's current medical follow-up status.

If no antiretroviral therapy was prescribed during pregnancy, indicate reason

- Select the appropriate response (check only one box).
- No prenatal care**-** mother did not receive any prenatal care
- HIV status of mother unknown**-** the provider may not have known her status because mother refused testing or was not offered testing
- Mother known to be HIV negative during pregnancy**-** She tested negative during her pregnancy and no additional tests were done to indicate seroconversion. Please note: a negative test during pregnancy must be noted in the medical chart
- Mother refused**-** She refused antiretroviral therapy during her pregnancy
- Other reason, specify**-** please specify why she did not receive antiretroviral therapy during her pregnancy

If no antiretroviral therapy was prescribed during labor & delivery, indicate reason

- Select the appropriate response (check only one box).
- Precipitous delivery/STAT c-section-The mother may abruptly deliver an infant which may preclude administration of antiretroviral therapy during labor and delivery
- Prescribed but not administered- the medication was ordered but it was not administered. This may be due to the hospital pharmacy not having the specific antiretroviral in stock. If the medication was prescribed but not given due to delivery prior to administration of the medication please mark box for 'Prescribed but not administered'
- HIV status of mother unknown**-** the provider may not have known her status because mother refused testing or was not offered testing
- Birth outside of hospital- If the birth occurred outside of the hospital, antiretroviral medication probably would not have been administered
- Mother known to be HIV negative during pregnancy**-** She tested negative during her pregnancy and no additional tests were done to indicate seroconversion. Please note: a negative test during pregnancy must be noted in the medical chart
- Mother refused**-** She refused antiretroviral therapy during her pregnancy
- Other reason, specify**-** please specify why she did not receive antiretroviral therapy during her pregnancy

If no antiretroviral therapy was prescribed for the infant during the first six weeks of life, indicate reason

- Select the appropriate response (check only one box).
- HIV status of mother unknown**-** the provider may not have known her status because mother refused testing or was not offered testing
- Mother known to be HIV negative during pregnancy**-** She tested negative during her pregnancy and no additional tests were done to indicate seroconversion. Please note: a negative test during pregnancy must be noted in the medical chart
- Mother refused**-** She refused antiretroviral therapy during her pregnancy
- Other reason, specify**-** please specify why she did not receive antiretroviral therapy during her pregnancy

Was substance use during pregnancy noted in the medical or social work records

- Select the appropriate response
- Information may be found in progress notes, social work notes, prenatal records and lab results

If yes, indicate which substances were used during pregnancy

- Select the appropriate response (Mark all that apply)
- Information may be found in progress notes, social work notes, prenatal records and lab results

Diagnosis (for the mother) of the following conditions during this pregnancy or at labor and delivery

- Select the appropriate response (Mark all that apply)
- Diagnosis of an STD may be found in prenatal records, progress notes and labs
- Bacterial vaginosis- clinician diagnosis. sometimes abbreviated as BV
- Chlamydia trachomitis infection- Lab tests include: culture,DFA, EIA, DNA probe, PCR, Nucleic Acid Amplification (NAAT), SDA (Strand Displacement Amplification), TMA (RNA Amplification).
- Genital Herpes- If she has primary herpes (first episode) or recurrence during pregnancy or at labor and delivery. Lab tests include: herpes virus culture, herpes cytology (herpetic inclusion bodies, cytology, inclusion body stain, Tzanck smear, Giemsa stain viral study), direct immunoflourescent AB or EIA, HSV Ag, PCR
- Gonorrhea (Neisseria gonorrhea)- Lab tests include: culture, DNA probe, PCR, SDA (Strand Displacement Amplification), TMA (RNA Amplification), Nucleic Acid Amplification (NAAT), Gram Stain
- Group B Strep- Group B streptococci. Screening for Group B strep occurs during 35 to 37 weeks in pregnant women
- Hepatitis B- Hepatitis B surface antigen, HbsAg. Women are usually screened during their initial prenatal visit or at time of labor/delivery. The test result should be for the surface antigen (HbsAg) rather than the antibody (anti-HBs), core antigen (HbcAg) or antibody (anti-HBc) or Hepatitis B e antigen (HbeAg) or antibody (anti-HBe)
- Hepatitis C-Lab tests include EIA screen followed by a recombinant immunoblot assay (RIBA)
- PID- Pelvic inflammatory disease. Clinician diagnosis
- Syphilis- Treponema pallidum. Lab tests include: For screening-VDRL, RPR and ART; For definitive diagnosis- DFA, EIA, IGG, IGM, DNA PCR, FTA-ABS, Darkfield microscopy, TP-PA.
- Trichomoniasis- Trichomonas vaginalis. Diagnosed by finding trichomonas on a wet mount

XVI. Comments

- Include any additional comments on the case in this section. Enter only comments that are pertinent to HIV surveillance.
- Please note that comments are not transmitted to the CDC.

APPENDIX 1: Document Source Codes

A01 Inpatient Record

A01.01	IPR/Acute Care Facility
A01.02	IPR/VA Hospital
A01.03	IPR/Military Hosp
A01.04	IPR/Long Term Care Fac
A01.05	IPR/Hospice

A02 Outpatient Record

A02.01	OPR/HMO
A02.02	OPR/VA Clinic
A02.03	OPR/Private Physician
A02.04	OPR/Adult HIV Clinic
A02.05	OPR/Infect Disease Clinic
A02.06	OPR/County Health Depart Clinic
A02.07	OPR/Maternal HIV Clinic
A02.08	OPR/Prenatal Clinic
A02.09	OPR/Pediatric HIV Clinic
A02.10	OPR/OBGYN
A02.11	OPR/Pediatric Clinic
A02.12	OPR/TB Clinic
A02.14	OPR/Indian Health Service
A02.15	OPR/Early Interv Nurse
A02.16	OPR/Visiting Nurse Service
A02.17	OPR/Hemophilia Trmnt Center
A02.18	OPR/Hospice
A02.19	OPR/Drug Treatment Center
A02.20	OPR/Rehabilitation Center
A02.25	OPR/Other Clinic

A03 ER Record N/Resulting in Admission

A04 Screening,Diagnosis,Referral

A04.01	SDR/Blood Bank
A04.02	SDR/Drug Treatment Clinic
A04.03	SDR/Family Planning Clinic
A04.04	SDR/HIV Case Management Agency
A04.05	SDR/HIV Counseling, Testing Site
A04.06	SDR/Immigration
A04.07	SDR/Insurance Report
A04.08	SDR/Job Corps
A04.09	SDR/Military
A04.10	SDR/Partner Counseling Service
A04.11	SDR/STD Clinic
A04.12	Public Health Notes

A05 Laboratory

A05.01	Laboratory/Hospital
A05.02	Laboratory/State
A05.03	Laboratory/Private

A06 Other Database

A06.01	OD/AIDS Drug Assist Prog ADAP
A06.02	OD/ASD
A06.03	OD/Birth Certificate
A06.04	OD/Birth Defects Registry
A06.05	OD/Cancer Registry
A06.06	OD/Database Provided by Coroner
A06.07	OD/Death Certificate
A06.08	OD/EHRAP
A06.09	OD/EPS
A06.10	OD/HARS
A06.11	OD/Health Department Records
A06.12	OD/Hepatitis Registry
A06.13	OD/Hosp Bill/Discharge Records
A06.14	OD/HRSA HIV Care
A06.15	OD/Immunization Registry
A06.16	OD/Medicaid Records
A06.17	OD/NDI Search
A06.18	OD/Out of State Reports
A06.19	OD/Prison, Jail, Oth Correc Fac
A06.20	OD/PSD
A06.21	OD/State Disease Registry
A06.22	OD/SHAS
A06.23	OD/SHDC
A06.24	OD/STD Registry
A06.25	OD/Tuberculosis Registry
A06.27	OD/Vital Statistic State/Local
A06.28	OD/HARS NDI
A06.50	OD/Other

A07 Other Facility Record

A07.01	OFR/Prison, Jail, Oth Correc Fac
A07.02	OFR/Coroner
A10	Other Source
A10.01	COPHI Investigation

APPENDIX 2: State Abbreviations

Abbreviation	State
AK	Alaska
AL	Alabama
AQ	American Samoa
AR	Arkansas
AZ	Arizona
BQ	Navassa Islands
CA	California
CO	Colorado
CQ	Mariana Island
CT	Connecticut
DC	District of Columbia
DE	Delaware
FC	Foreign Country
FL	Florida
FM	Micronesia
GA	Georgia
GQ	Guam
HI	Hawaii
IA	Iowa
ID	Idaho
IL	Illinois
IN	Indiana
JQ	Johnston Atoll
KS	Kansas
KY	Kentucky
LA	Louisiana
MA	Massachusetts
MD	Maryland
ME	Maine
MI	Michigan
MN	Minnesota
MO	Missouri
MQ	Midway Island
MS	Mississippi
MT	Montana
NC	North Carolina
ND	North Dakota
NE	Nebraska
NH	New Hampshire
NJ	New Jersey
NM	New Mexico
NQ	Trust Territories
NV	Nevada
NY	New York
OH	Ohio
OK	Oklahoma
OR	Oregon
PA	Pennsylvania
PR	Puerto Rico
RI	Rhode Island
RM	Marshall Island
RQ	Puerto Rico
SC	South Carolina
SD	South Dakota
TN	Tennessee
TX	Texas
UT	Utah
VA	Virginia
VQ	Virgin Islands
VT	Vermont
WA	Washington
WI	Wisconsin
WQ	Wake Island
WV	West Virginia
WY	Wyoming

APPENDIX 3: Extended Races

Extended Races
Central American
Cuban
Dominican
Mexican
Puerto Rican
South American
Spain/Portugal
Chinese
Filipino
Japanese
Korean
Asian Indian
Vietnamese
Laotian
Thai
Cambodian
Pakistani
Indonesian
Hmong
Burmese
Bangladeshi
Sri Lankan
East Indian
Malayan
Okinawan
Taiwanese
Singaporean
Pacific Islander
Samoan
Tongan
Tahitian
Guamanian
North Mariana
Palauan
Fijian
Micronesian
Alaska Native
Aleut
Eskimo Indian
American Indian
Cajun

APPENDIX 4: Facility Types

Code	Facility Type
F.OTH	(F.OTH) Facility/Other
F.UNK	(F.UNK) Facility/Unknown
F01	(F01) Inpatient Facility [IP Fac]
F01.01	(F01.01) IP Fac/Hospital
F01.04	(F01.04) IP Fac/Long Term Care
F01.50	(F01.50) IP Fac/Drug Treatment
F01.OTH	(F01.OTH) IP Fac/Other
F01.UNK	(F01.UNK) IP Fac/Unknown
F02	(F02) Outpatient Facility [OP Fac]
F02.01	(F02.01) OP Fac/HMO Clinic
F02.03	(F02.03) OP Fac/Prvt Physician's Office
F02.04	(F02.04) OP Fac/Adult HIV Clinic
F02.05	(F02.05) OP Fac/Infectious Disease Clinic
F02.09	(F02.09) OP Fac/Ped HIV Specialty Clinic
F02.10	(F02.10) OP Fac/OBGYN Clinic
F02.11	(F02.11) OP Fac/Pediatric Clinic
F02.12	(F02.12) OP Fac/TB Clinic
F02.16	(F02.16) OP Fac/Home Health Agency
F02.17	(F02.17) OP Fac/Hemophilia Trmnt Center
F02.18	(F02.18) OP Fac/Hospice
F02.19	(F02.19) OP Fac/Drug Treatment Center
F02.25	(F02.25) OP Fac/Other Clinic
F02.50	(F02.50) OP Fac/ACTG Site
F02.51	(F02.51) OP Fac/Community Health Center
F02.52	(F02.52) OP Fac/Employee Health Clinic
F02.53	(F02.53) OP Fac/Hlth Dpt/Pub Hlth Clinic
F02.54	(F02.54) OP Fac/Mobile Clinic
F02.55	(F02.55) OP Fac/Non-mobile Street Outrch
F02.56	(F02.56) OP Fac/PACTG Site
F02.57	(F02.57) OP Fac/Pri Care Clinic, N/Spec
F02.58	(F02.58) OP Fac/School or Univ Clinic
F02.OTH	(F02.OTH) OP Fac/Other
F02.UNK	(F02.UNK) OP Fac/Unknown
F03	(F03) Emergency Room
F04	(F04) Screening/Diagnostic/Referral [SDR]
F04.01	(F04.01) SDR/Blood Bank/Plasma Center
F04.02	(F04.02) SDR/Drug Treatment Center
F04.03	(F04.03) SDR/Family Planning Clinic
F04.04	(F04.04) SDR/HIV Case Mgmt Agency
F04.05	(F04.05) SDR/HIV Counseling, Testing Site
F04.07	(F04.07) SDR/Insurance Screening
F04.11	(F04.11) SDR/STD Clinic
F04.OTH	(F04.OTH) SDR/Other
F04.UNK	(F04.UNK) SDR/Unknown
F05	(F05) Laboratory
F07	(F07) Other Specific Facility [OS Fac]
F07.01	(F07.01) OS Fac/Correctional Facility
F07.02	(F07.02) OS Fac/Coroner or Med Examiner

APPENDIX 5: AIDS Indicator Diseases

AIDS INDICATOR DISEASES
Candidiasis, bronchi, trachea, or lungs
Candidiasis (esophageal)
Carcinoma (invasive cervical)
Coccidioidomycosis (disseminated or extra-pulmonary)
Cryptococcosis (extra-pulmonary)
Cryptosporidiosis, Chronic Intestinal >1 month duration
Cytomegalovirus Disease (other than in liver, spleen, or nodes)
Cytomegalovirus Retinitis (with loss of vision)
HIV Encephalopathy
Herpes Simplex: chronic ulcers >1 month duration or bronchitis, pneumonitis, or esophagitis
Histoplasmosis (disseminated or extra-pulmonary)
Isosporiasis - chronic intestinal >1 month duration
Kaposi's Sarcoma
Lymphoma Burkitt's (or equivalent term)
Lymphoma Immunoblastic (or equivalent term)
Lymphoma, primary in brain
Mycobacterium avium complex or M kansasii, (disseminated or extra-pulmonary)
M tuberculosis, pulmonary
M tuberculosis, (disseminated or extra-pulmonary)
Mycobacterium of other species or unidentified species, (disseminated or extra-pulmonary)
Pneumocystis carini pneumonia
Pneumonia, recurrent, 12 month period
Progressive mulitfocal leukopencephalopathy
Salmonella septicemia, recurrent
Toxoplasmosis of the brain
Wasting syndrome due to HIV

Appendix H:
Abbreviated ACRF For STD*MIS

Instructions for Completing the Abbreviated ACRF For STD*MIS

Purpose of the Form

- This is an abbreviated version of the ACRF that can be used by HIV surveillance staff to complete information that they find in STD*MIS on an existing case.

Report status

- This should only be used to provide updates for existing cases.

Note: If the case has never been reported, you must provide a full ACRF on the case. You can conduct a medical record review and use the abbreviated ACRF for STD*MIS to provide updated information from STD*MIS. Alternatively, you can complete a full ACRF from STD*MIS (not using this form), but at a later date you must also review the cases medical record at the facility of diagnosis or care.

TDCJ Case

- Check the box for cases known to be in a TDCJ facility at the time of ACRF completion.

Stateno

- If the ACRF is for a "New Case", assign a unique stateno.
- If the ACRF is for an "Update to AIDS" or "Other Update", fill in the eHARS stateno which has already been assigned.
  - **NOTE**: The eHARS stateno should be used for ALL "Update to AIDS" cases – even if the case is progressing from HIV to AIDS in a different jurisdiction. "Update to AIDS" cases will not be assigned a new stateno, even if the case was diagnosed with AIDS in a different jurisdiction.

I. Form Information

- All information in the form section of the ACRF must be filled out to be considered a complete report.

Document Source

- The Document Source has been pre-selected as A06.24 (STD Registry).

Report Medium

- The Report Medium has been pre-selected Paper Form, Field Visit.

Surveillance Method

- The Surveillance Method has been pre-selected Follow-up.

Date Form Completed

- Enter the date on which you completed this form.

Person Completing Form

- Enter the name of the person completing this ACRF.
  - For surveillance staff, enter your three letter initials only (e.g. MRF).

- For staff who are not surveillance staff (e.g. staff at a clinic), enter your entire name (Last Name, First Name) including your credentials (e.g. MD).

Facility where Information was obtained

- The Facility where Information was Obtained has been pre-completed as "STD*MIS".

II. Name

Name Type

- Select the appropriate name type for each name completed and complete the full name of the case. See the list below for available name types.
- For a "New Report", the legal name must be on the form.

Name Type	Description
Legal	Person's legal name
Alias	Person's assumed name
Maiden	Person's name immediately before a first marriage; in most cases, equal to birth name
Married	Name assumed from a partner in a marital relationship
Nickname (Call me)	Person's preferred name when directly addressed, such as a nickname or street name
Birth	Person's name at birth
License	Person's name when granted a license to practice a profession or when issued a formal certificate
Display	The name displayed in a system (for example, a hospital's medical records system) as the primary name for a patient
Indian/Tribal	Person's Indian, indigenous, or tribal name
Professional	Person's professional name, such as a pseudonym or pen name, or an abbreviation of a professional organization or title entered in the Suffix field
Religious	Person's religious name instead of a secular name
Record	Person's officially written and preserved name on record, such as in judicial proceedings

Name

- Include all available name parts (first, middle, last, prefix, and suffix). Spell the name exactly as it appears in the document source, including any punctuation like dashes (-) or apostrophes (').
- If there are more than two names in one document source, list the additional names and their corresponding name type in the Comments section.

III. Current Address

Address Type

- Select the appropriate address type for the most current address listed in the document source being reviewed. Below is a list of address types available in eHARS.

Address Type	Description
Residential	Address of a residence
Correctional	Address of a correctional facility (including jails)
Homeless	Address of a location where a homeless person spends most of their time. Homeless should only be used with documented evidence that the patient is homeless and not because an address could not be found.
Foster home	Address of a foster home
Bad address	Address is known to be for a place that does not exist.
Postal	A PO box address or the address of a mail receipt facility
Residence at death	Person's residence at time of death
Residence at birth	Person's residence at time of birth
Shelter	Address of a shelter
Temporary	Address of a short term (temporary) residence

Address

- Enter the patient's most current address listed in the document source being reviewed. Be sure to enter the patient's complete address, including street address and zip code.
- If the patient is homeless, record the zip code for the where the person spends most of their time. If this information is not available then enter the zip code for where the person was tested.
- Since eHARS can accommodate more than one address, if a patient has a temporary address or is only temporarily residing in a shelter or correctional facility you should also record the patient's residential address if available. Additional addresses should be recorded in the Comments section, including the address type.

IV. IDs

- List all patient IDs and corresponding ID type. List any additional IDs in the comments section, including the type of ID.

ID Type

- Select the appropriate ID type. Below is a list of ID types available in eHARS.

ID Type
Medical Record Number
OOS Stateno
Prison Number
RVCT (TB) Number
Social Security Number (SSN)
Social Security Number Alias
STD*MIS Number

- For OOS (out of state) cases, include the two letter abbreviation of the other state in the ID type field "other." Use the format <two letter state abbreviation> stateno (e.g. "LA stateno").

ID

- Enter the full ID for each ID type selected.

V. Demographic Information

Diagnostic status

- Select the diagnostic status of the case.

Sex at Birth

- Select the sex of the patient at birth. If the patient's current sex is different than their sex at birth, note this in the Comments section.

Date of Birth / Alias Date of Birth

- Enter the patient's date of birth as it appears in the document source. If the date of birth is known to be an alias date of birth, then complete the alias date of birth field with this date of birth.

Country of Birth

- Check the appropriate box. For cases not born in the USA, write in the full name of the country of birth.

Vital Status / Date of Death / St of Death

- Check the appropriate vital status box. If the case is deceased, the date of death and state of death fields must be completed. Use the state's two letter abbreviation. Use the code "FC" (foreign country) for cases whose place of death is outside of the United States. Refer to *Appendix 2: State Abbreviations* for a list of the two letter state codes.

Ethnicity

- Check the appropriate box. If ethnicity cannot be found, then select "Unknown."

Race

- Check the appropriate box or boxes. If race cannot be found, then select "Unknown."

Extended Race

- If you know the extended race of a case then complete this field using one of the extended races listed in *Appendix 3: Extended Races*.

VII. Personal History

- Complete all questions of the personal history section by selecting "Yes", "No" or "Unknown".
- Select "Yes" if you find documented evidence in that document source that the person has that risk factor.
- Select "Unknown" if the personal history is truly unknown after reviewing all of the information in the document source.
- Only select "No" if you find documented evidence that the person does not have the risk factor (e.g. the medical record states "patient has never injected drugs").

- If you select received clotting factor, complete the clotting factor type and date received.

Heterosexual Relations with any of the following

- This section should only be completed if the case has had documented heterosexual contact. For male cases, you must have checked "yes" for sex with female. For female cases, you must have checked "yes" for sex with male.
    - For males, you should NEVER select "Yes" to "Heterosexual contact with a bisexual male", since this biologically infeasible.
- Only select "Yes" to the last four options in the Personal History section if this risk factor might be the primary mode of HIV exposure for this case. In other words, you should select "Yes" to these four questions, if the case is believed to have acquired HIV through one of these risk factors. For example, if a case reports that they report that they had a blood transfusion, but they are a known MSM then you would not respond to the transfusion question. **Selecting one of these risk factors will initiate a COPHI investigation.**
- Do not select "Yes" to the blood transfusion or transplant questions if the transfusion or transplant occurred outside the United States.
- Only select "Yes" for Worked in a health care or clinical laboratory setting if this was the primary mode of transmission. If the patient is not believed to have acquired HIV through their healthcare work then you should not select "Yes" to this risk factor.
- If other documented Risk is selected, write in the risk factor.

XI. Treatment

- Complete the treatment section by selecting the appropriate check boxes.

For Women:

- Complete the For Women section if applicable.

For Child:

- Enter each child separately.
- Enter the child's name, stateno and date of birth.
- Enter the hospital of birth, with the appropriate address information.
- If you identify information on more than 1 child, this information should be completed in the Comments Section by including all information listed above.

VIII. Testing and Treatment History Information

General Guidance

- Surveillance sites are required to complete the TTH data elements on the ACRF for all newly reported adult HIV cases.
- When doing an STD*MIS abstraction, if you find any mention of testing or treatment history (TTH) in the STD*MIS record, please record the information on the abbreviated ACRF for STD*MIS. However, you do not need to report on this form information reported in the TTH fields within the interview record, since this information will be imported directly from STD*MIS into eHARS.

- This section of the ACRF is the only section where patient self-reported information is acceptable.
- The following are descriptions of the common response options for the TTH data elements:

Response	Description
Yes	Indicates that there was sufficient documented evidence that the event occurred. Evidence can be from patient self-report, health care provider note, or laboratory documentation.
No	Indicates that there was sufficient documented evidence that the event did not occur. Evidence can be from patient self-report or health care provider documentation of no previous negative test.
Unknown	Indicates that the patient reported "don't know", the health care provider documented "unknown", or there was insufficient documented evidence for or against (supporting or denying) the occurrence of the event.
Refused	Indicates patient refused, health care provider recorded "refused", or facility refused to permit the medical record review.
Blank	Indicates that the usual data sources were not investigated and/or the health care provider/staff were not asked.

Main Source of Testing and Treatment History Information

- Select the appropriate box to indicate the source of information for the TTH form. If the source of data is unknown, then leave blank.

Source Type	Description
Provider Report	Information was obtained from a report submitted by a health care provider or from a phone call with a provider. Information was found by the provider from chart notes, laboratory reports, or recollection from discussion with the patient or another health care provider.
Patient Interview	Patient was directly asked these questions by DIS, a counseling and testing provider or someone who has received some training in the proper collection of TTH information
Medical Record Review	Health Department staff obtains the information through review of medical charts or electronic medical record.
Other	Information was obtained from another

	source.

- Only one box may be checked per form. If information comes from more than one source, then additional ACRF forms, one for each source, should be completed.

Date Patient Reported Information

- Fill in month, day and year completely.
- The variable represents different dates, depending on the circumstances in which the information was primarily obtained.

Source Type	Date Patient Reported Information
Patient Interview	Date of interview
Medical Record Review	The last date of the patient encounter or provider's note that contributed to the TTH information reported in this ACRF. Do not use the actual medical record review date unless there is no other date to use.
Provider Report	The date when most of this information was obtained from the patient or another data source, or, lacking that, the date when the provider completed the report.
Other	The date information was obtained from another source.

- Do not leave this date blank. This date will be used for prioritizing the selection of incidence data in eHARS person view when there are multiple TTH documents. If the date patient reported information is unknown, enter the date when the document was received at the health department.

Ever had a previous positive HIV test?

- This provides information about the patient ever having a positive HIV test before the current test.
- Answer with the response Yes, No, Unknown, or Refused as described in general guidance above.

Date of First Positive HIV test

- This is the date of the earliest known positive HIV test for the patient. This date could be from an anonymous test that will never be reported to the national HIV surveillance system.
- Enter the date (MM/DD/YYYY) of the **first positive** HIV test. If the day is unknown, enter the MM/../YYYY. If the month is unknown, leave the month blank and just enter the year (YYYY).
- For the TTH section of the ACRF, this date is often self-reported.
- Do not report indeterminate or false positive tests.

Ever had a negative HIV test?

- Check whether the patient has ever tested **negative** for HIV. Answer with the response Yes, No, Unknown, or Refused. See general guidance above.
- Self-reported information is acceptable.

- If yes, then enter the date (MM/DD/YYYY) of the **last negative** test. If the day is unknown, enter MM/../YYYY. If the month is unknown, leave the month blank and just enter the year (YYYY).
- If the individual never had a negative HIV test prior to the first positive test mark "No"
- Unknown should only be marked if the patient did not know if s/he has ever tested negative or all potential sources of information were reviewed and there was no information about the patient's negative tests history.
- Last negative refers to a negative confirmatory test.
- If Unknown is marked, **do not** answer the next question "Number of negative HIV tests within 24 months before first positive test"

Number of negative HIV tests within 24 months before first positive test (do not include first positive test)

- The purpose of this variable is to indicate testing frequency in the 24 months before the first positive HIV test in order to calculate the inter-test interval for repeat testers where there is no date of last negative test. Indicate the number of times the patient has tested in the **24 months** before his/her first positive test.
- This question is often misinterpreted. Note that:
    1. Include only tests during the 24 months prior to the first positive test, whenever it was.
    2. By definition, prior tests must be negative because they come before the first positive.

    Examples:
    1. If a patient's first positive test was today and he indicates that he tested negative three other times in the past 24 months, his total will be 3 tests.
    2. If a patient's first positive test was also his first ever test, his total will be 0.
    3. If a patient had five negative tests in his lifetime, but only two were in the 24 months before the first positive then the total would be 2.

Has the patient ever taken any Antiretroviral medications?

- Check whether the patient has taken any antiretroviral (ARV) medications prior to his/her first positive test. This includes highly active-antiretroviral therapy (HAART) or ARV, some medications for hepatitis, and post-exposure prophylaxis for HIV. Self-reported data are acceptable.
    - If yes, then list the medications.
    - If yes, then indicate the start date (MM/DD/YYYY). If exact date is unknown include the month and year or just year.
    - If yes, then indicate the end date (MM/DD/YYYY). If exact date is unknown include the month and year or just year.
    - If the patient is currently taking medications and has not completed the regimen check the Currently Taking check box and leave the end date field blank.
-

IX. Local Fields

- Please note that Local fields are not transmitted to the CDC.

Prison Facility

- If the person was in prison at the ACRF was completed, enter the name of the correctional facility in the Correctional Facility local field. If a case was moved from one correctional facility to another, both correctional facilities can be indicated here. Separate multiple facilities with a ";"

Partner's Name

- Enter any Partner's Names for the case. If multiple partners are identified, separate with a ";". Please ensure that the order of Partner's Name to Partner's Stateno is retained. If you do not have a Partner's Name but you have a Partner's Stateno, enter N/A in the Partner's Name field.

Partner's Stateno

- Enter any Partner's Stateno's for the case. If you have multiple partner's Stateno's, separate with a ";". Please ensure that the order of Partner's Name to Partner's Stateno is retained. If you do not have a Partner's Stateno but you have a Partner's Name, enter N/A in the Partner's Stateno field.

Previous HIV History

- If you identify previous unreported HIV history, such as diagnoses prior to 1999, enter this information.

Lab Name of First Positive Test

- For all "New Case" reports, enter the name of the lab that conducted the confirmatory HIV lab test for this case report form. For example, if the lab conducting the EIA is different from the lab conducting the Western Blot, you should enter the name of the lab conducting the Western Blot. If the laboratory name is not known, complete this field with "UNKNOWN". This field should be completed for all new cases.

X. Comments

- Include any additional comments on the case in this section. Enter only comments that a pertinent to HIV surveillance.
- Please note that comments are not transmitted to the CDC.

Appendix I

(Death Report Form not included. Please contact your local HIV Surveillance program to request information about the death report form)

Instructions for completing the Death Report Form

Many of the fields on the Death Report Form are also seen in the ACRF. Often times, the directions for completing a field on this form will be the same as completing the same field on the ACRF. However, be mindful of potential differences in the possible responses, as there may be slight variations.

Stateno:

- Fill in the eHARS stateno associated with the case.

TDCJ Case:

- Check whether the case was known to be in a TDCJ facility at the time of death

I. Form Information

As with the ACRF, the form information section must be completed in order to be considered a complete death report.

Document Source:

- The options listed are the only options available for entry into a death report form.
  Note: Death information gathered from medical records abstractions should not be used to complete this form. The death report form is reserved for instances where one receives a specific death report. Any death information found during an abstraction should be entered on an ACRF.
- Check the one box corresponding to the document type used to fill out the form. Information gathered from a second data source needs to be reported on a separate death report form.

Potential Source	Description
A06.06	Database Provided by Coroner
A06.07	Individual Death Certificate
A06.27	Local Vital Statistics
A06.30	Social Security Death Index or Master File

Death Certificate #:

- If available, enter the death certificate number. If not available, leave the field blank.

Report Medium:

- The medium through which you found information about the case's death. See the table below for selecting the appropriate response:

Medium	Description
Field Visit	Information gathered at a facility
Mailed	Facility directly mailed information
Telephone	Spoke with facility over telephone to gather information

Electronic	Information sent electronically by facility (ex. Downloading files from FTP site)

Surveillance Method:

- The method through which you found information about the case's death. See the table below for selecting the appropriate method:

Method	Description
Active	You INITIATED process to gather information. Example: you asked your local vital statistics office for all deaths due to HIV, and you find HIV cases not previously reported.
Passive	You receive information on deaths WITHOUT having requested it. Example: A facility calls to notify you of a new HIV death, and you had not previously asked for this information
Follow-up	You obtain information on a previously reported case. A large majority of death reports will be considered follow-up.

Date Form Completed:

- Enter the date on which you completed the death report form. Two digits are reserved each for the month, day, and year of completion. Use the last two digits of the current year to represent the year of completion.

II. Name

Name Type:

- Select the appropriate name type for each name completed and complete the full name of the case. See the list below for available name types:

Name Type	Description
Legal	Person's legal name
Alias	Person's assumed name
Maiden	Person's name immediately before a first marriage; in most cases, equal to birth name
Nickname	Person's preferred name when directly addressed, such as a nickname or street name
Married	Name assumed from a partner in a marital relationship
Other	If none of the above categories fit the name type listed on the source document, select this box and write in the name type listed on the source document

Name:

- Include all available parts of the name (first, middle, last, prefix, and suffix). Spell the name exactly as it appears in the source document, including any punctuation, such as apostrophes (‘) and hyphens (-).
- If there are more than two names in one source document, list the additional names and their corresponding name type in the “Comments” section.

III. Address

Address type:

- Mark the appropriate type of address for the current address listed on the source document (this address may or may not differ from place of death information). Below are the types of addresses available on the death report form:

Address Type	**Description**
Residential	Address of a residence
Correctional Facility	Address of a correctional facility (including jails)
Homeless	Address of a location where a homeless person spends most of their time. Homeless should only be used with documented evidence that the patient is homeless and not because an address couldn’t be found.
Postal	A PO box address or the address of a mail receipt facility
Temporary	Address of a short term (temporary) residence
Other	If the current address does not fit into any of the above types, mark this field and write the best characterization of the address type on the source document

Address:

- Enter the patient’s most current address listed in the source document being reviewed. Be sure to enter the patient’s complete address, including street address and ZIP code.
- If the patient is homeless, record the ZIP code for where the person spends most of their time. If this information is not available, then enter the ZIP code for where the person died.
- Since eHARS can accommodate more than one address, if a patient has a temporary address or is only temporarily residing in a shelter or correctional facility you should also record the patient’s residential address if available. Additional addresses should be recorded in the Comments section, including the address type.

IV. ID

ID Type:

- Listed below are the different ID types available on the Death Report Form

ID Type
Social Security Number (SSN)
Social Security Number Alias
Prison Number
Medical Record Number
STD*MIS Number
RVCT (TB) Number
Other

- If an ID type is available on the source document that is not in the above list, mark "Other" and complete the ID type. If the ID type is an out-of-state stateno, also list the two-letter state abbreviation.

ID:

- Enter the full ID for each ID type selected.
- There is space for up to three different IDs listed on a single source document. Additional IDs should be recorded in the Comments section along with the corresponding ID type.

V. Demographics

Date of Birth:

- Enter the case's date of birth as it appears in the source document. If the date of birth is known to be an alias date of birth, make note of this in the Comments section.

Date of Death:

- Enter the case's date of death as it appears in the source document.

Sex at Birth:

- Select the sex of the patient at birth. If the patient's current sex is different than their sex at birth, record this in the Comments section.

Ethnicity:

- Check the appropriate box. If ethnicity cannot be found, leave the field blank.

Race:

- Check the appropriate box or boxes. If race cannot be found, leave the field blank.

VI. Place of Death Information

This section is reserved for information on the place where the case died; this is different from the case's residence/current address when they died. If the information is not available on the source document, leave the fields blank.

City of Death:

- Enter the city where the case died as listed on the source document.

State of Death:

- Enter the state where the case died as listed on the source document.

County of Death:

- Enter the county where the case died as listed on the source document.

Country of Death:

- If a case died within the United States, mark the USA box. If the case died outside the United States, mark the Other box and write the name of the country where the case died.

Place of Death:

- Listed below are the different potential places of death available in eHARS:

Places of Death
Hospital, inpatient
Hospital, outpatient or emergency room
Hospital, dead on arrival
Nursing home or hospice
Residence
Jail/Adult detention center
Juvenile detention center
Group/assisted living home
Homeless shelter
Homeless, on the street
*Hospital, institution (HARS)**

*** Note that even though this is a possible selection, it should not be used**

- If a place of death is indicated but does not fit into any of the above categories, mark the Other box; there is no need to describe this place of death in detail. If a place of death is not indicated on the source document, mark the Unknown box.

VII. Cause of Death Information

Autopsy:

- Indicate whether a case received an autopsy after death.
- Mark Yes or No if the information is available from your source. If the information is not listed on the source document or not available, mark Unknown.

Additional Cause of Death (ICD-10):

- This field captures ICD-10 codes connected to a case's cause(s) of death.
- Enter each cause of death into a separate series of boxes in the same order as the information is shown on the source document. If the information is not available, leave the fields blank.
    - If the ICD code on the document is three digits (ex: B20), use the three connected boxes to the left of the decimal point. Leave the box after the decimal point blank.
    - If the ICD code on the document is four digits (ex: B21.1), write the first three digits into the boxes left of the decimal point and the fourth digit to the right of the decimal point.

- There is space available for up to 14 unique ICD-10 codes. If a subject has more than 14 codes listed in their file, you can use the Comments field to include the remaining codes.

Comments:

Use this sections for any overflow responses or any extra notes written on the source document. If you do not have enough space to write overflow responses, attach additional comments on a separate sheet. If you attach a separate sheet to the death report form, make sure to include the Stateno at the top of the extra sheet.

Appendix J:
Electronic Data Transfer Instructions

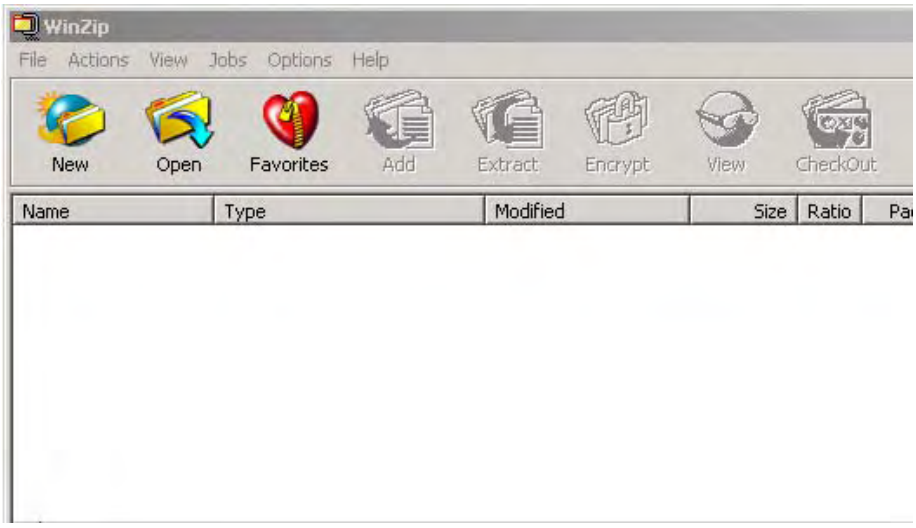
Electronic Data Transfers

It is exceedingly important to ensure that all data is encrypted and sent to Central Office through secure mediums (See Chapter 7 for more information on security requirements). The following sections describe how to zip, encrypt, unzip and decrypt files using WinZip and how to use the TxPHIN web portal to safely transfer data to Central Office.

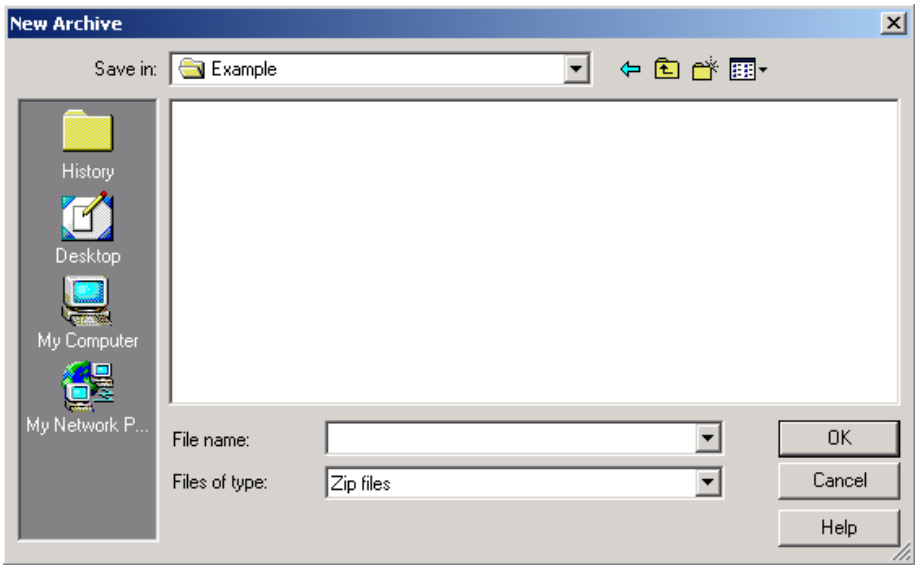
Using WinZip to compress files

Winzip is a tool to make working with Zip files and other types of archive files easier. Archives are files that contain other files, and Zip files are the most common format. The files in an archive are compressed. Winzip uses the term "Add" to mean "compress files and add them to an archive".

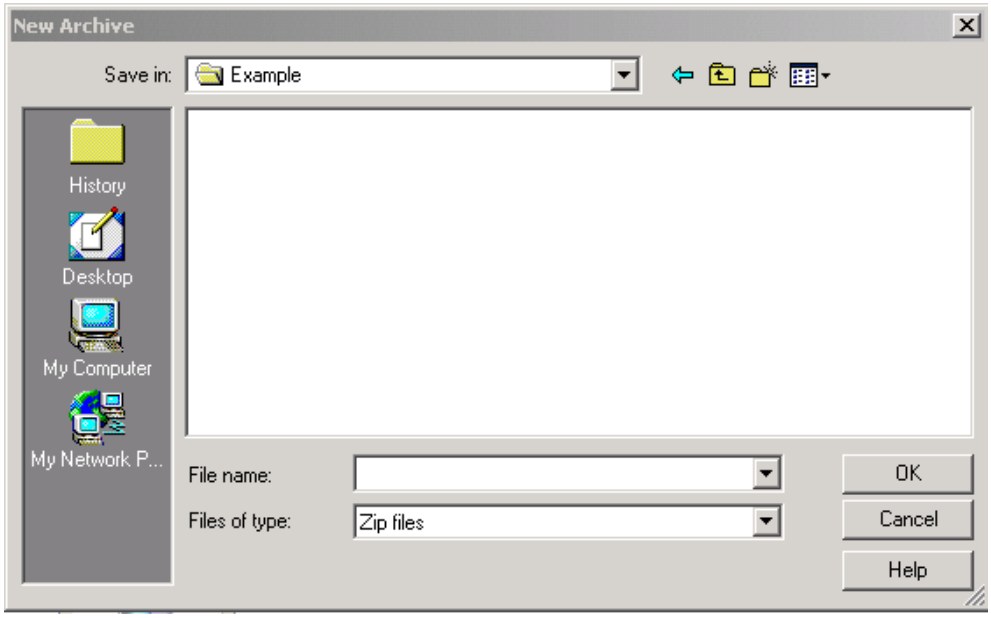
1) Click on Winzip Icon to Open



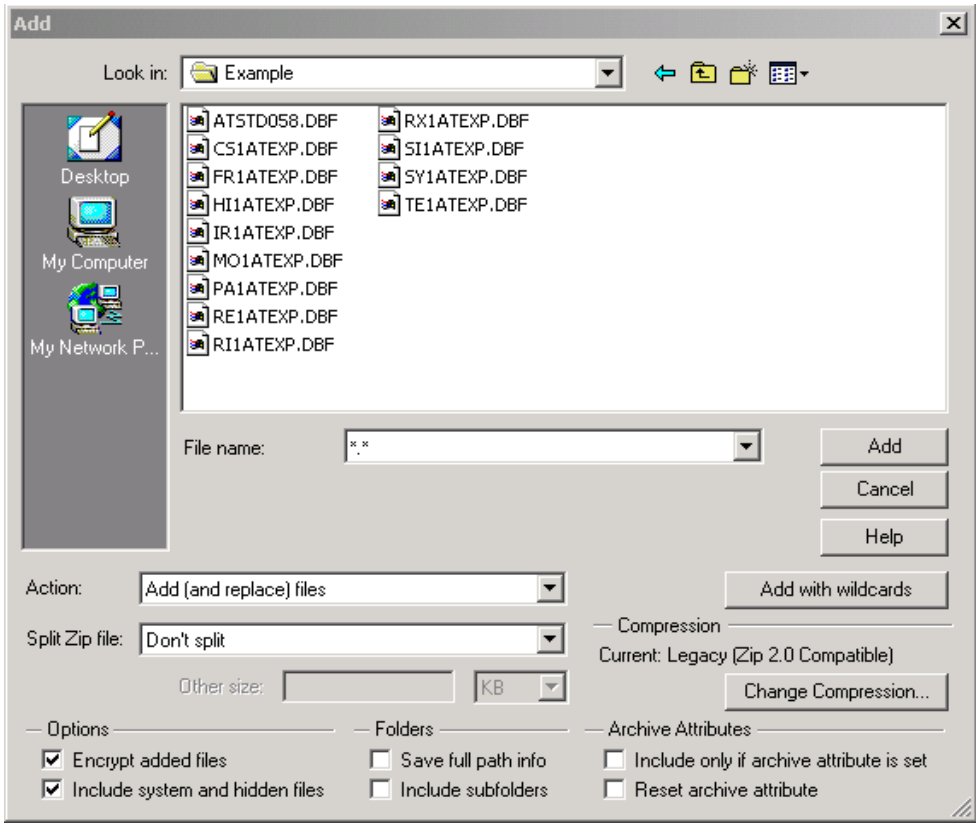
2) Go to Menu Bar and *select* **File**
3) In the pull-down menu, *select* **New Archive** (see screen below)



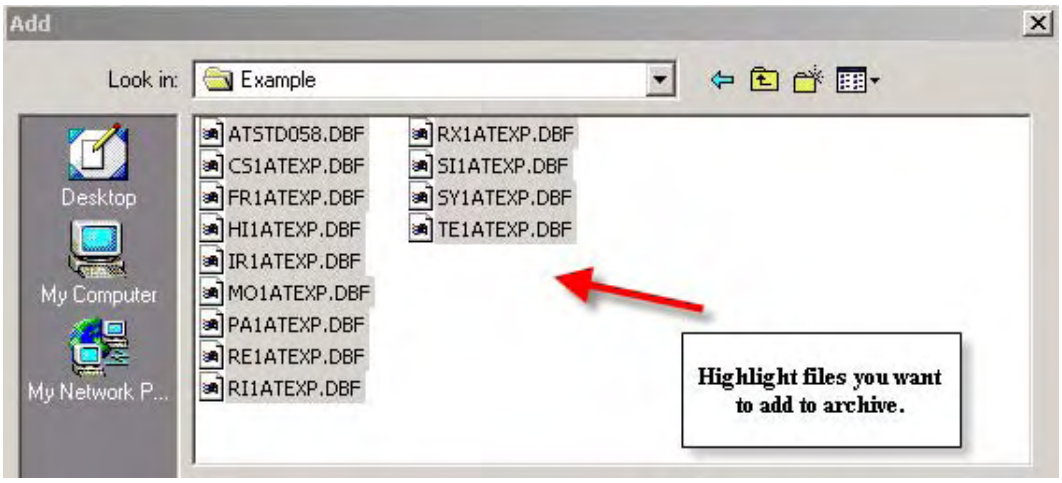
4) In the **File name:** box, type the name of the archive/zip file you want to create. *Do not enter the names of the files you want to compress/zip*.
5) In the **Save in:** box, choose the drive and folder where the archive/zip file will be created. (see screen below)



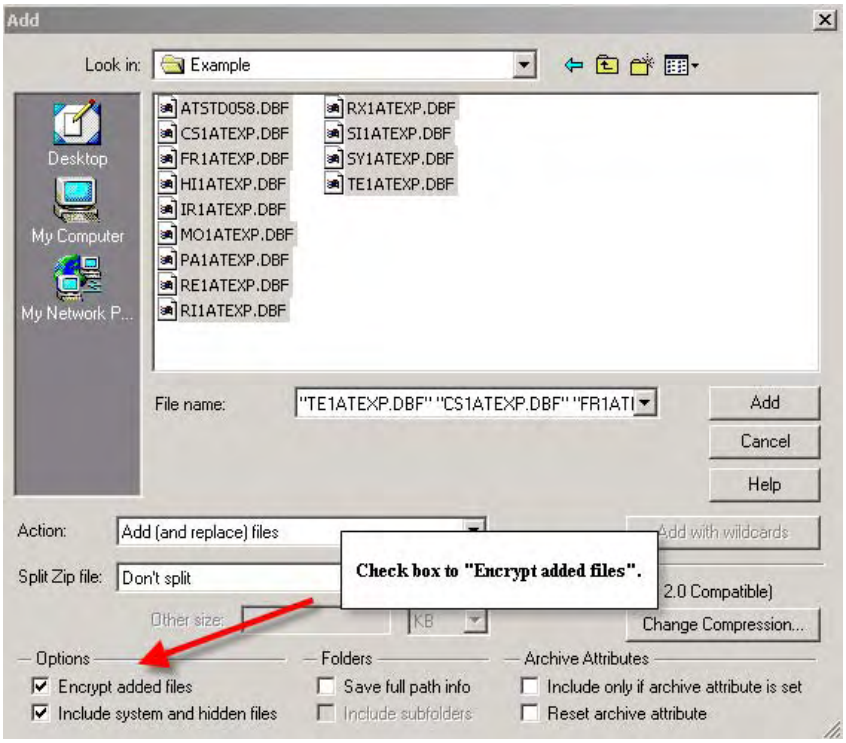
6) In the **Files of type:** box, *select* Zip files
7) Next, *click* the **OK** box to go to the *Add window*
8) You should now see the **Add** window (see screen below)



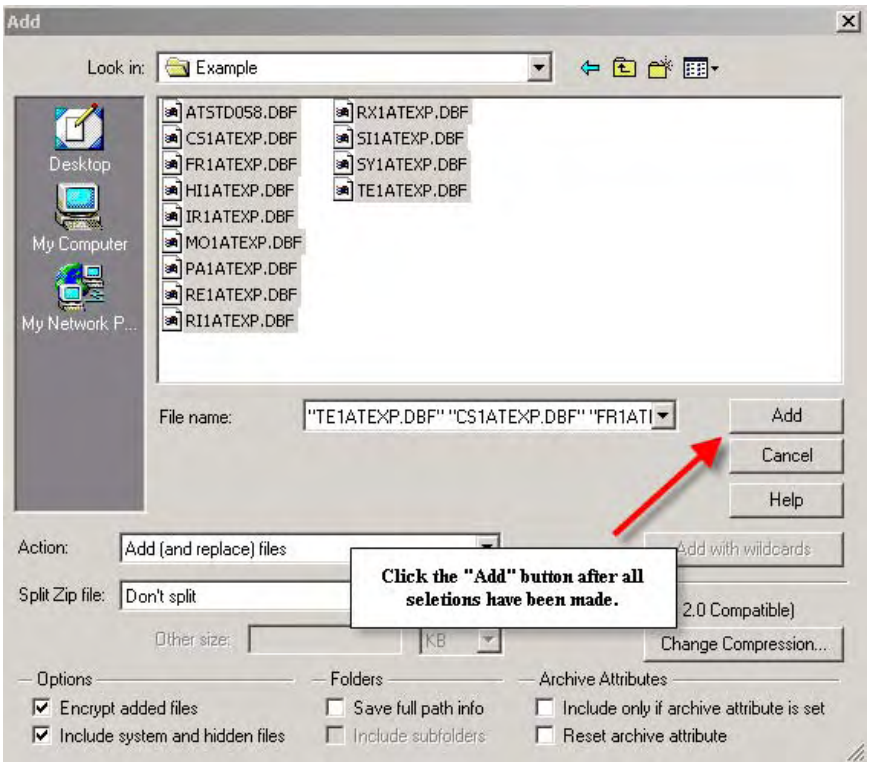
9) In **Look in:** box, select drive and folder where the files are located you want to add to the zip file.
10) In the Add window, *select* the files by highlighting the ones you would like to add to the archive file. (see screen below)



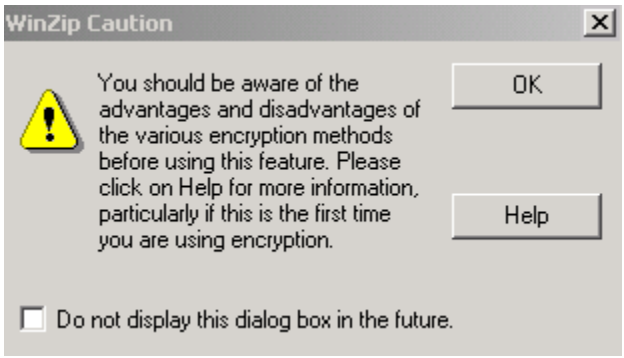
11) In **Options**, located in the bottom left corner of Add window, check Encrypt added **files** box.


Add
Look in:
Example
Desktop
My Computer
My Network P...
ATSTD058.DBF
CS1ATEXP.DBF
FR1ATEXP.DBF
HI1ATEXP.DBF
IR1ATEXP.DBF
MO1ATEXP.DBF
PA1ATEXP.DBF
RE1ATEXP.DBF
RI1ATEXP.DBF
RX1ATEXP.DBF
SI1ATEXP.DBF
SY1ATEXP.DBF
TE1ATEXP.DBF
File name:
"TE1ATEXP.DBF" "CS1ATEXP.DBF" "FR1ATI
Add
Cancel
Help
Action:
Add (and replace) files
Add with wildcards
Split Zip file:
Don't split
Check box to "Encrypt added files".
2.0 Compatible)
Other size:
KB
Change Compression...
Options
Encrypt added files
Include system and hidden files
Folders
Save full path info
Include subfolders
Archive Attributes
Include only if archive attribute is set
Reset archive attribute

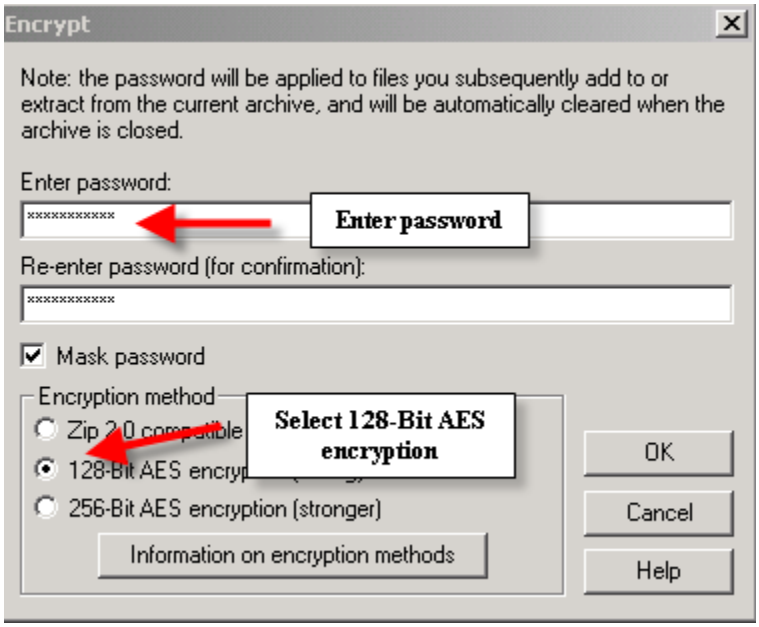
12) *Click* the **Add** button after all selections have been made.



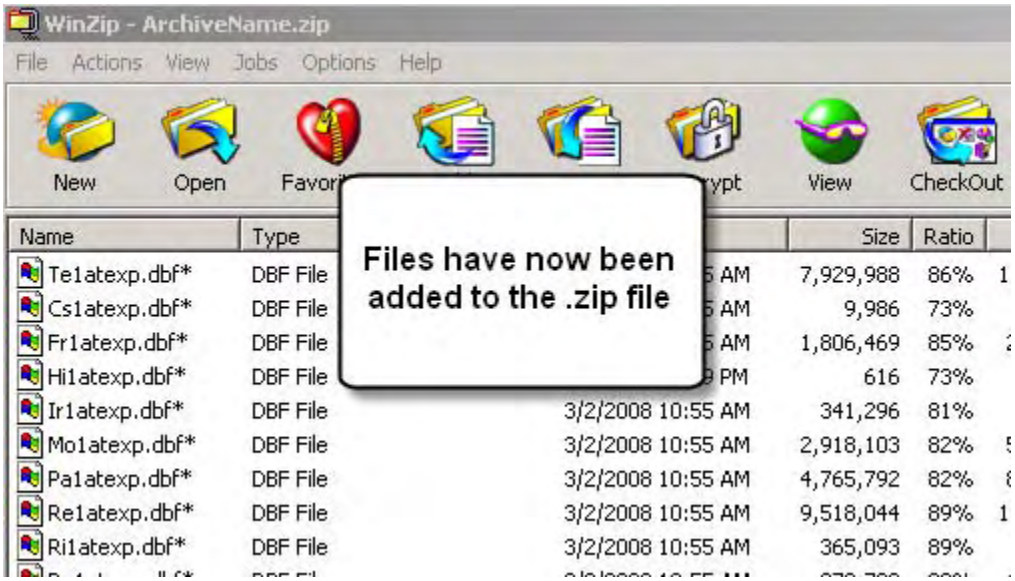
13) You will now see the screen below, *click* **OK**.



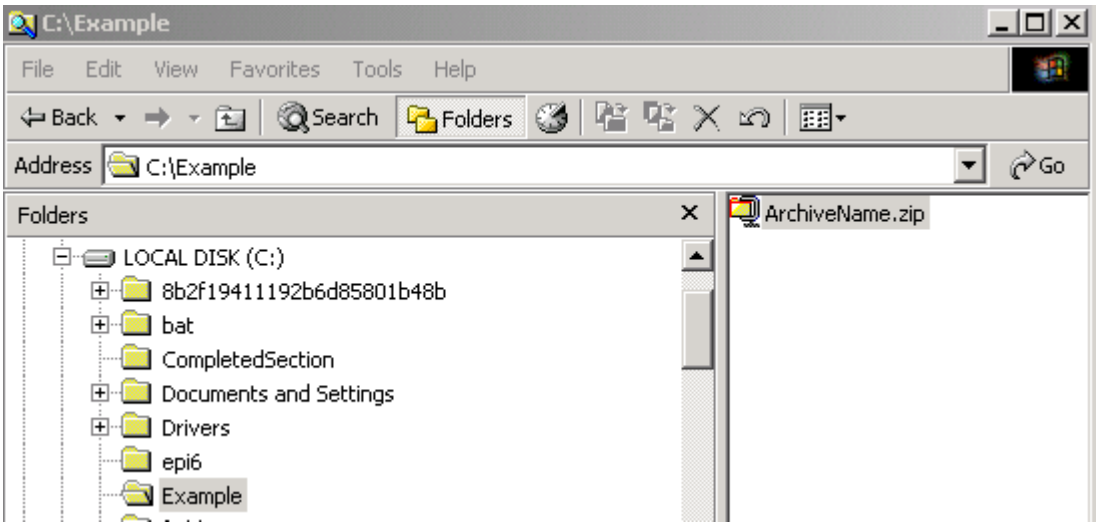
14) Enter password for the ****.zip file, see screen below.



15) *Click* **OK** button



16) Go to where you specified the new archive/zip file to be created. You should now see the .zip file listed. *See example screen below.*



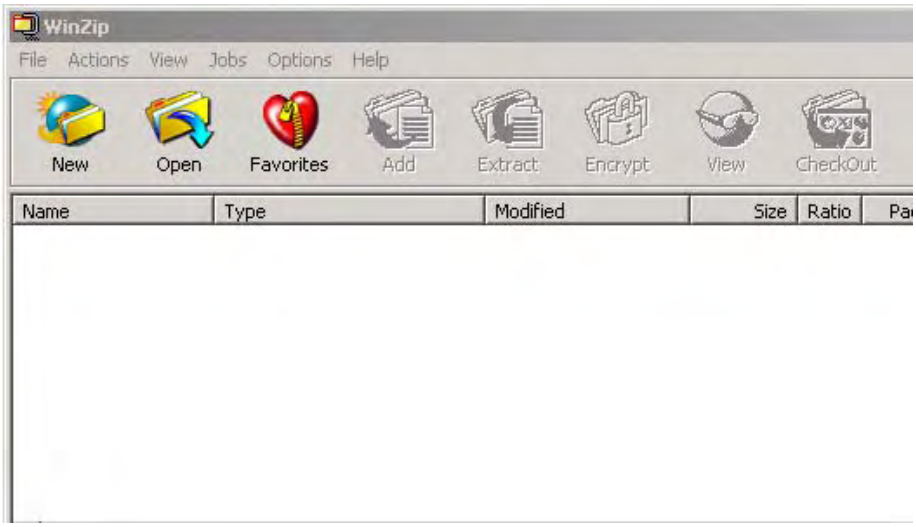
17) You are now ready to upload the .zip file via TxPHIN.

You have now compressed files into a new archive using Winzip. There are other ways to compress files into a new archive. For introductory information, please see the section Brief Tutorial – Creating New Archives in Winzip "Help".

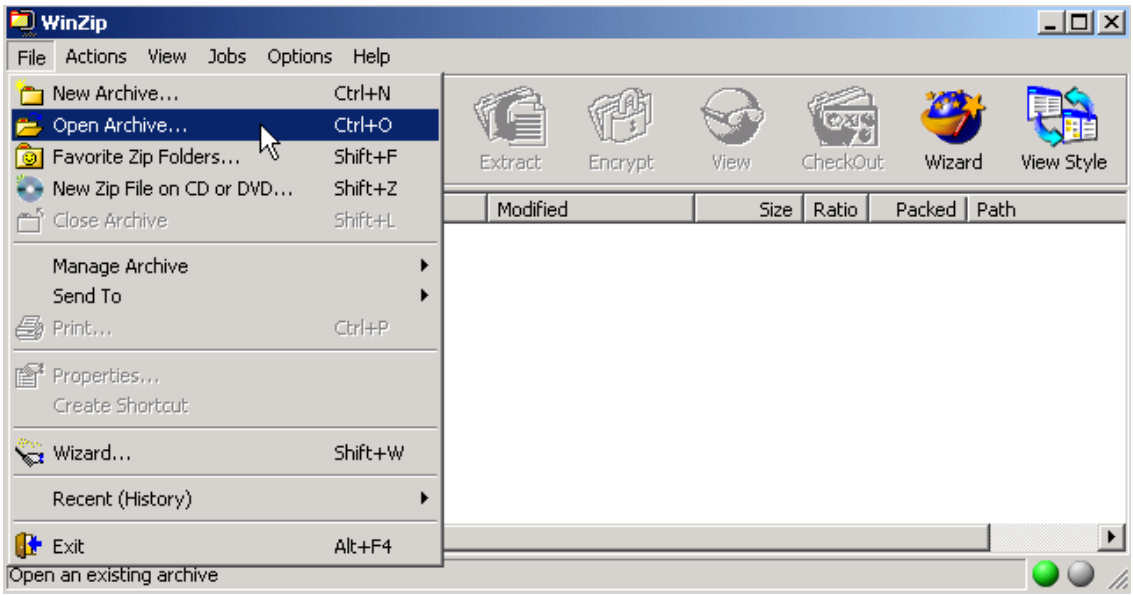
Using WinZip to extract files

Winzip is a tool to make working with Zip files and other types of archive files easier. Archives are files that contain other files, and Zip files are the most common format. The files in an archive are compressed. Winzip uses the term "Extract" means "decompress files in an archive, creating separate files on a disk or folder".

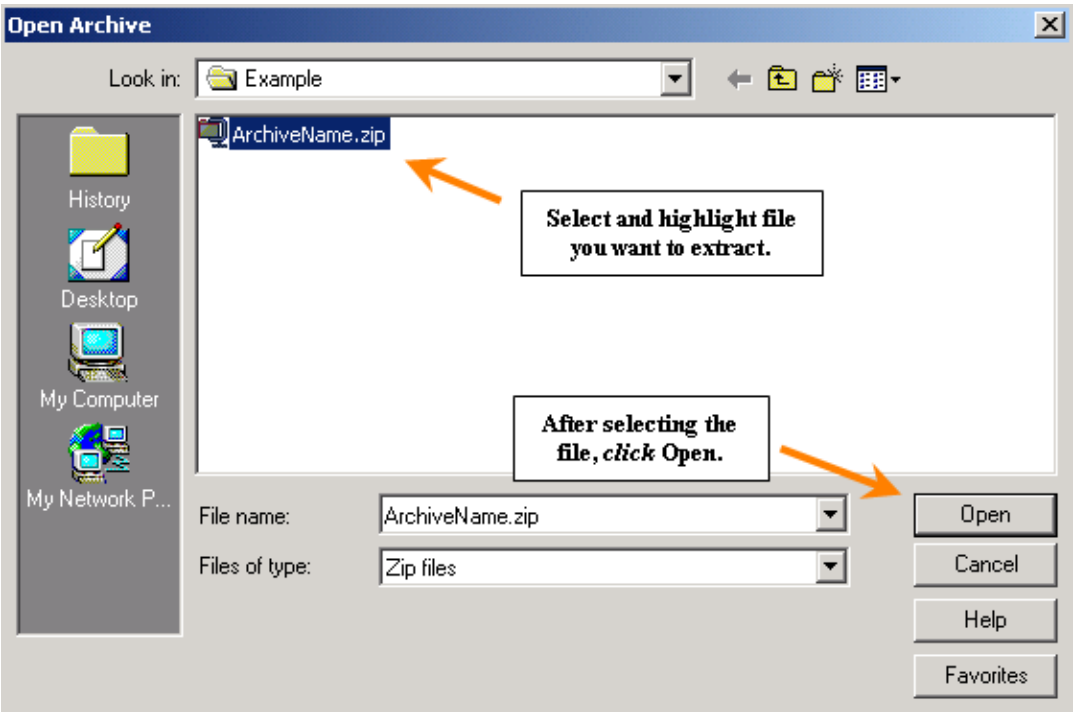
18) Click on Winzip Icon to Open



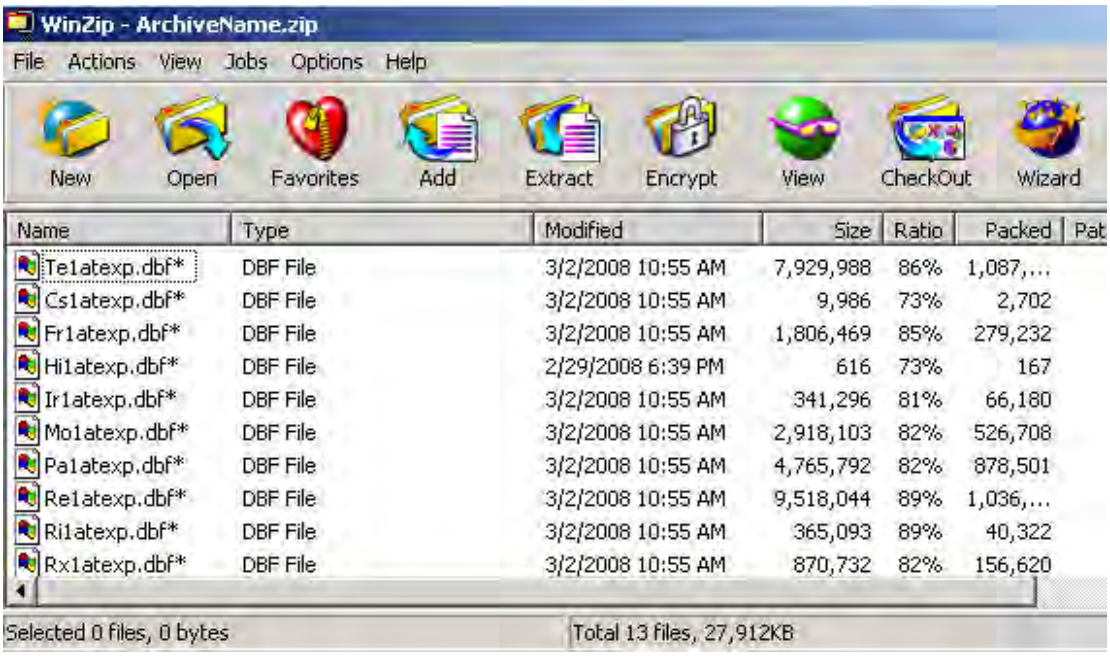
19) Go to Menu Bar and *select* **File**
20) In the pull-down menu, *select* **Open Archive** (see screen below)



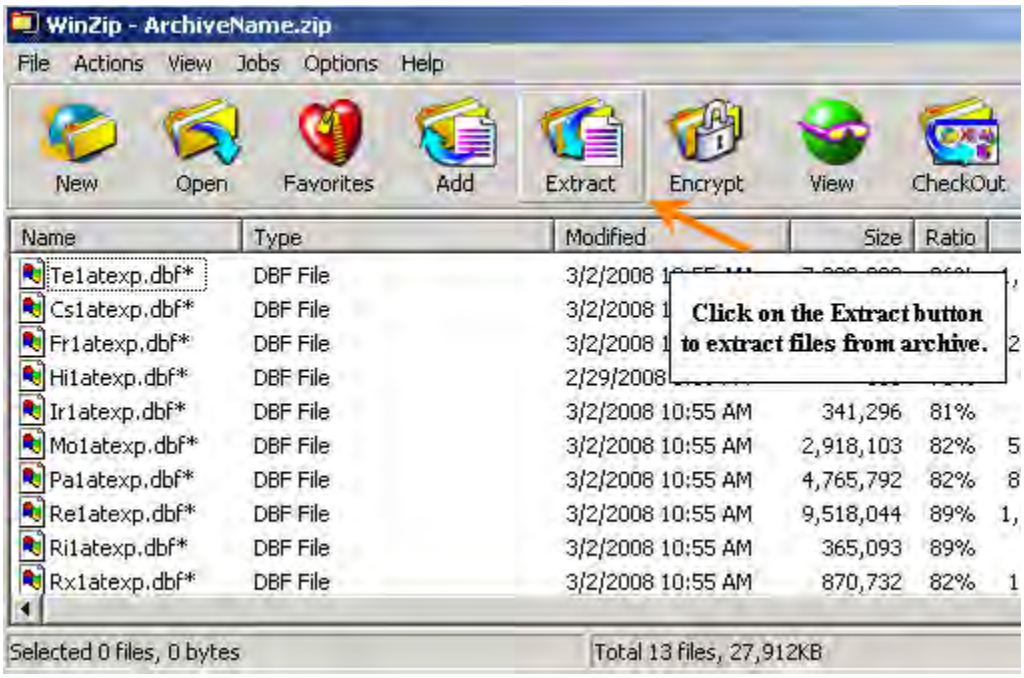
21) In the **Look in:** box, browse to find the compressed file (.zip) you wish to extract. Select and highlight the #####.zip file. (See screen below)
22) *Click* Open. (See screen below)



23) After you open the ****.zip file. Winzip will list the compressed files in the ****.zip file. (see screen below)

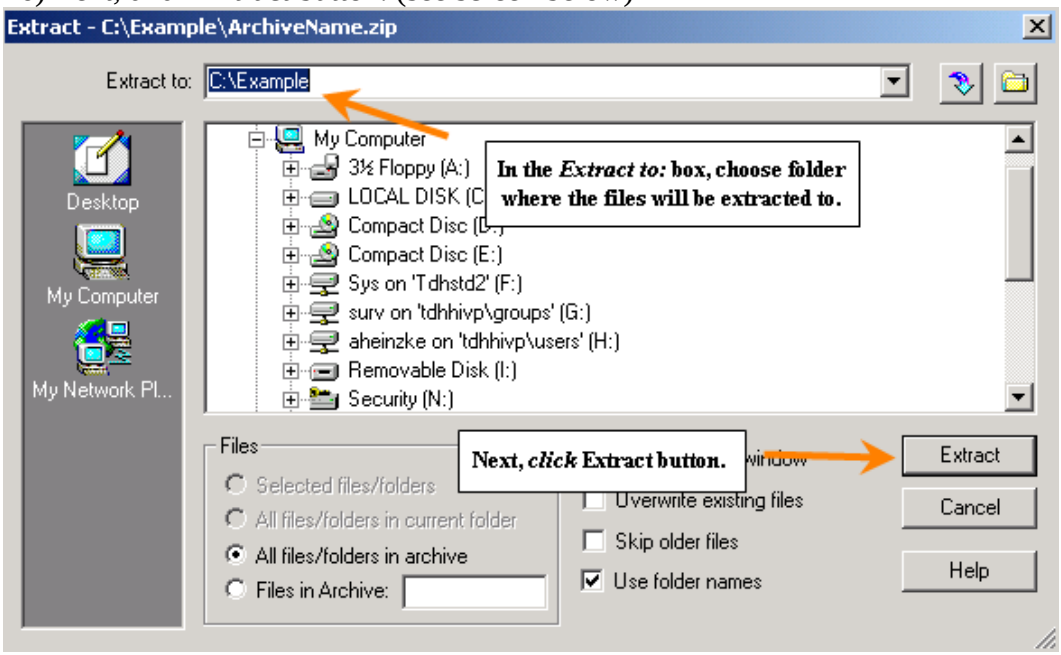


24) Next, click the "Extract" button to extract the files from the archive (see screen below)

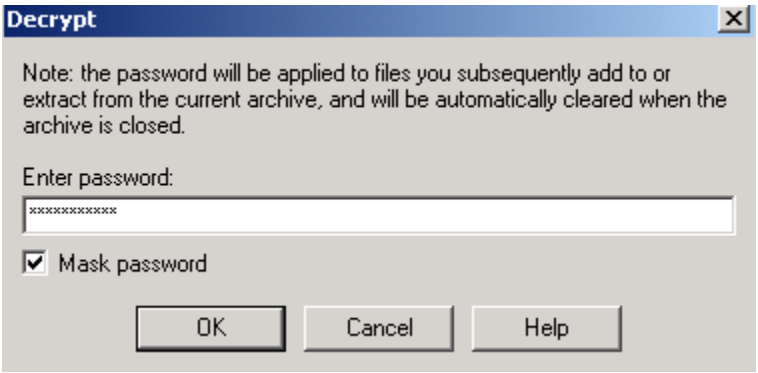


25) In the **Extract to:** box, choose folder or location to extract the files too.

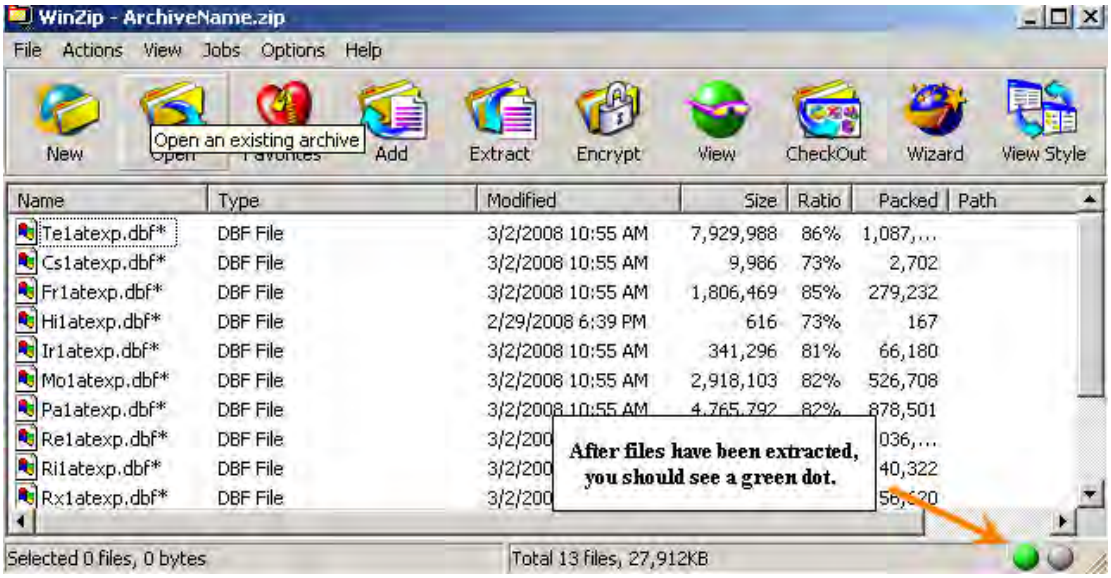
26) Next, *click* Extract button. (see screen below)



27) Enter password, if archive file is encrypted.
28) Next, *click* OK. (see screen below)

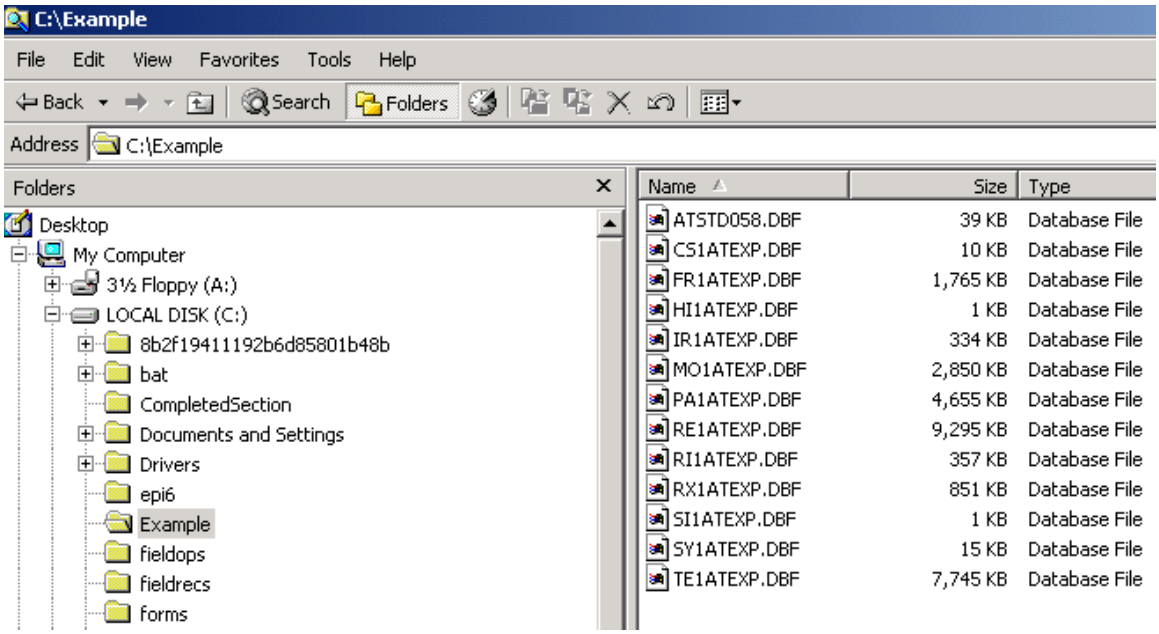


29) After files have been extracted, you should see a green dot at the bottom of the Winzip window. This indicates that the extraction process is complete. (See screen below)



30) All files should now be extracted to the location you specified.

31) Goto Windows Explorer and choose the specified folder. You should see the extracted files listed. (See screen below)

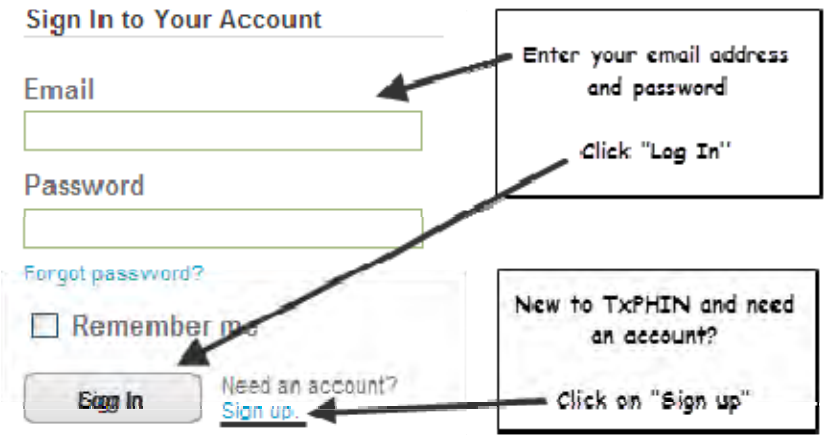


You have now extracted data from a compressed file using Winzip. There are other ways to extract files from an archive. For introductory information, please see the section Brief Tutorial – Extracting Files in Winzip "Help

GAINING ACCESS TO THE TEXAS PHIN PORTAL

To access the Texas PHIN, go to the website at https://www.txphin.org

On the front page you will be asked to sign in to your account. This will require you to have a username and password.



New to TxPHIN; you will need to create an account. Click on the link labeled "Sign Up"; located to the right of the "Log In" button.

Your browser will be directed to a form on which you should fill in the required information: First Name, Last Name, Email Address, Password and Role - Communicable/Infectious Disease Coordinator.

Please take the time to fill in the optional information as well. Listed below are the different profile attributes the form requests:

Language: Check your preferred language as either English or Spanish.
Job Title: Please provide your job title so administrators can better decide what roles to grant you.

Home Jurisdiction: When choosing your Home Jurisdiction, from the drop down box click on the county or DSHS Health Service Region that you operate in for your job. If you have responsibility for statewide activities that are not limited to a certain county or region, click on "Texas". Your choice of jurisdiction is very important. The portal presents content and functionality based on this attribute. For example, it is possible for

jurisdiction administrators to load news content that specifically pertains to their county. If you are not registered in that county, you won't see that custom, localized content.

Requesting a Public Health Professional Role Be Assigned to You: Access to applications and features within the Texas PHIN portal is highly dependent upon what Roles are assigned to your user profile. Check the box next to the question "Public Health Professional?". When the box is checked more form fields will appear. Scroll through the list of Roles and click on the one that best describes your designated role in public health or emergency activities. You do not have to choose a Role. You will automatically be assigned the Role of Public if you do not choose a different Role. You will have the opportunity to request more Roles after gaining access to the portal.

Professional Organization: If you are affiliated with any of the professional organizations listed in the next drop down box, click on the appropriate organization. If you are not affiliated, you do not have to choose an organization.

Role: Briefly describe your role in your organization. This information will assist administrators in evaluating your user application and deciding to grant Roles to your user profile.

Select – "Communicable/Infectious Disease Coordinator in Texas" as one of your roles.

(This role is for using TxPHIN for the DSHS HIV/STD Surveillance Department)

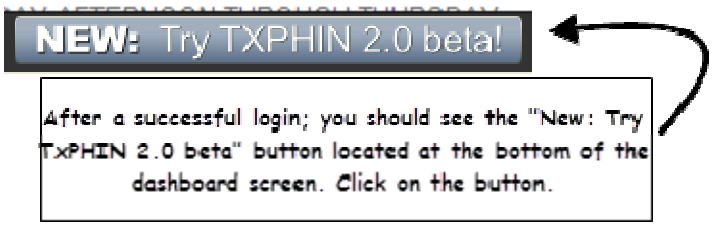
Lastly, click on the Submit button when you have entered all required information. After submitting the registration you will receive an email from the phinadmin@txphin.org asking you to confirm your email address by clicking the link within the email.

You will also receive an email confirming your Role assigned by the PHIN administrator. This role is the public health professional role you choose during the registration process.

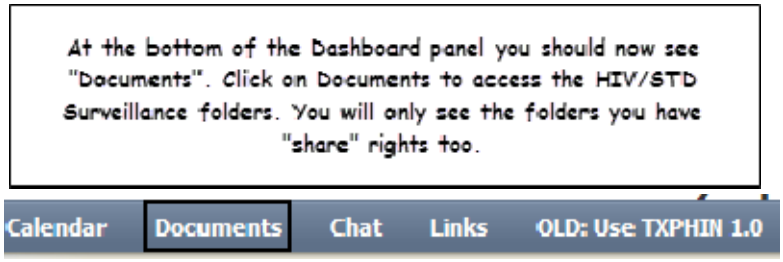
Once you have confirmed your email address you will be directed to the Texas PHIN webpage.

After a successful login; you will see the Dashboard. The Texas PHIN Dashboard is the main navigation page that allows you to see and share information, update your profile and able to transfer documents.

The documents panel is located in the "NEW: Try TxPHIN 2.0 beta!" version. Click on the 2.0 beta version button to go to the documents panel.



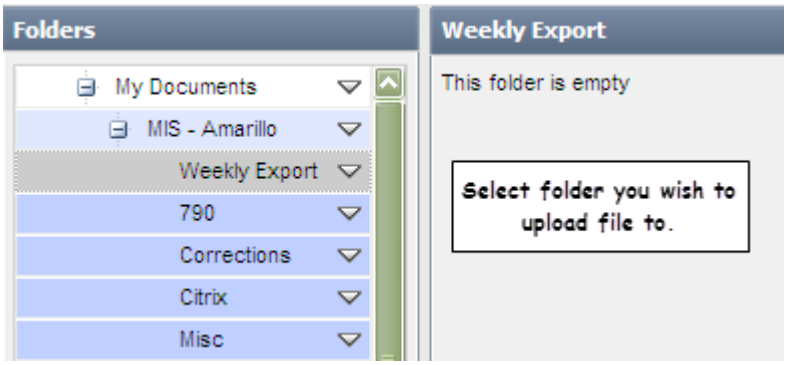
After clicking on the 2.0 beta version button located at the bottom of the dashboard panel; you now should see the Documents link. Click on "Documents" to access the folders. Users will only see folders that they have "share" rights too.



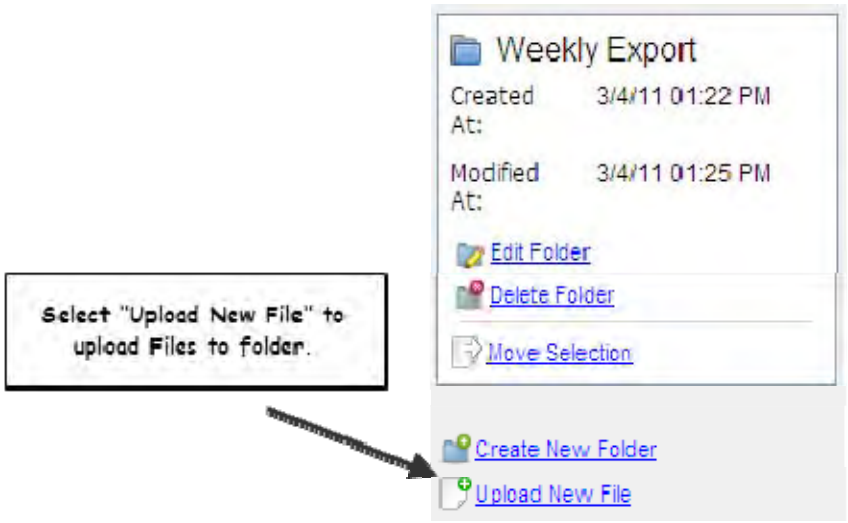
The documents panel; located on your dashboard, allow you to upload, download and share files across the PHIN.

Uploading a file into a folder

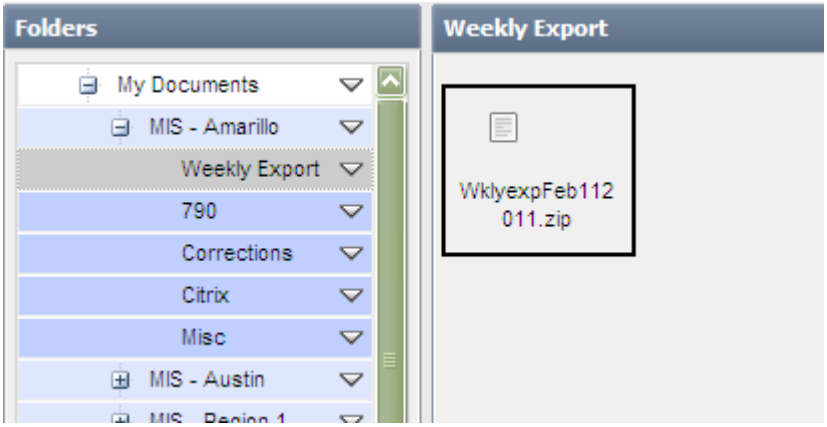
1.) Locate and click on the folder you wish to upload a file to.



2.) Locate and click on the "Upload New File" located in the right side panel to upload files.



The file you uploaded should now appear in the folder you selected.



Downloading a file from the documents panel

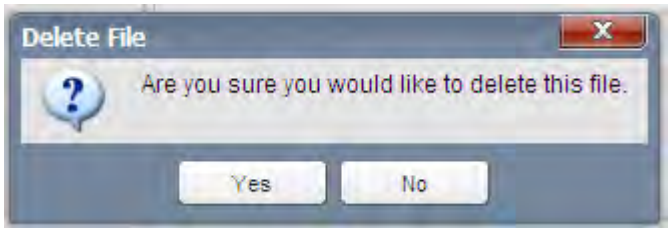
1.) Locate and select file you wish to download. Click on "Download File".

2.) After clicking on "Download File", you will be asked to save the file to a location of your choice. Browse to a destination folder and click save.

Deleting a file from the documents panel

1.) Locate and select file you wish to delete. Click on "Delete File" link to delete file.

2.) Select "yes" if you are sure you want to delete file.



For assistance; you may call Alan Heinzke, Terry Donohoo or Stan See.

<u>MIS/ICCR folders:</u>

Alan Heinzke – alan.heinzke@dshs.state.tx.us – (512) 533-3027

<u>ELR Folders:</u>

Terry Donohoo – terry.donohoo@dshs.state.tx.us – (512) 533-3028

<u>HIV Folders:</u>

Stan See – stan.see@dshs.state.tx.us – (512) 533-3038

Chapter 2 Perinatal HIV Surveillance

2-1 General Overview

The purpose of Perinatal HIV Surveillance is to target and follow the progress toward maximal reduction of perinatal HIV transmission. Data is collected using the HIV/AIDS pediatric case report form (PCRF). A PCRF is completed for all live children born to HIV infected women (residents of Texas) regardless of the child's HIV status (indeterminate, infected, or seroreverter).

The data collected include: maternal prenatal care usage, maternal HIV test history, prenatal and neonatal antiretroviral therapy, other interventions to prevent transmission, receipt of prophylaxis and treatment by the infant, appropriate follow-up care of the mother and child, and other interventions relevant to the evaluation of recommended public health actions to prevent perinatal HIV transmission.

Perinatal surveillance consists of additional case ascertainment methods, linking of mother-infant pairs and review of supplemental medical records. Supplemental medical record reviews will include both the mother's and child's medical records (mother's HIV clinic chart, prenatal records, labor and delivery records, newborn hospital and pediatric clinic charts, birth and death certificates, and laboratory reports) to assess testing, prenatal care, treatment, longitudinal follow-up to assess infection status of infants, initiation of HIV-related care, and long-term outcomes. Matching HIV/AIDS and birth registries will be conducted to help ensure that all mother/infant pairs are identified and the data are representative of all HIV-infected pregnant women. Where feasible, additional registry matches (i.e. birth defects and tumor registries) will be conducted to assess potential adverse outcomes of antiretroviral exposure among infected and uninfected children in the short and long term.

HIV-exposed infants identified through perinatal surveillance will be followed up by the appropriate surveillance site every 6 months for up to 18 months until their HIV infection status is determined, and, if they meet the HIV/AIDS case definition, will continue to be followed to determine their vital status. Children found to be HIV-uninfected will be maintained in eHARS as a perinatal exposure.

2-2 Reporting/Ownership

Each surveillance site is responsible for completing a pediatric case report form for every child born within their jurisdiction. An exposure will belong to the jurisdiction where the woman was residing at the time of birth. If the child is born outside of the country or in another state to a woman residing in Texas, any available Texas medical records will be abstracted and a pediatric case report form will be completed. If the child changes residency and the diagnosis status is updated to HIV infected or AIDS, the exposure will change ownership to the new jurisdiction where the child was residing at the time of HIV or AIDS diagnosis.

2-3 Data Collection

Data for completing the pediatric case report form will be collected from various medical records including the following (as available or applicable):

a. Prenatal care records
b. Maternal HIV clinic records
c. Labor and delivery records
d. Pediatric birth records
e. Pediatric HIV medical records
f. Pediatric medical records (non-HIV clinic/provider)
g. Birth certificate
h. Death certificate
i. Health department records
j. Other records

A child should be reported into eHARS no later than 45 days after the child's date of birth. If care for either the mother or the child was received outside of the jurisdiction of residency, the surveillance site where care was received is responsible for abstracting any other pertinent information. It is the responsibility of each jurisdiction to communicate with other jurisdictions in order to assure all information necessary to complete the PCRF has been abstracted.

All pediatric medical records should be reviewed six weeks postpartum or later so that data on neonatal antiretroviral use, breastfeeding, etc. will be available. However, timely collection of these data is essential for identification of missed prevention opportunities, and targeting of prevention activities.

The maternal information pertinent to each pregnancy must be included. If a woman has twins or triplets, a separate PCRF should be completed for each infant.

2-4 Case Ascertainment

Surveillance staff must regularly contact reporting facilities or have an active reporting system established with delivery hospitals and clinics to identify potential/suspect HIV/AIDS perinatal exposure cases. HIV-infected women should be identified during pregnancy by surveillance staff and the infant should be followed-up until the infection status is known.

All reports of pregnant HIV positive women should be recorded using the tracking spreadsheet provided by DSHS. Further, when contact to prenatal care providers, HIV care providers for pregnant women, and pediatric HIV providers is made to identify HIV positive women and their infants, information should be tracked using the abstraction database provided by DSHS.)

Each surveillance site must maintain regular contact with health care practitioners from hospitals and clinics. (**One hundred percent of providers of HIV care to pregnant women must be contacted once every two months to discover if there are new HIV positive pregnant women in care and to obtain the estimated date of delivery.)** Perinatal exposures may be identified through the following strategies: 1.) Review of medical records of newly reported women of child bearing age suspected to be HIV positive, 2.) Communication between the surveillance sites and providers regarding women that have been previously identified as HIV positive and have since become pregnant, 3.) Review of laboratory results from rapid testing performed at delivery. 4.) Birth registry linkages (e.g. programs can match HIV cases in women of child-bearing age with the birth registry database annually).

1) For newly reported women of child bearing age who are identified as potential HIV positive cases prior to delivery, laboratory reports may be the primer for initiating an HIV/AIDS related surveillance investigation. Beginning with receipt of the lab report, surveillance staff should then perform a follow-up investigation involving the review of medical records for these newly reported women. When reviewing the medical record, surveillance staff must first review the record to confirm the woman's HIV status. For women who are identified as being infected, surveillance staff must also review the medical record looking for an indication that the woman is pregnant. If the woman is determined to be pregnant, the woman's information is entered into a local database, and the woman's prenatal care and HIV care is tracked until her delivery date. **(Reports of known pregnant HIV infected women must be provided to DSHS on a monthly basis.)**

2.) Perinatal exposures may also be identified through active surveillance involving communication between each of the surveillance sites and providers. This regular communication will pertain to women who have been previously identified as HIV positive and have since become pregnant. Staff from each of the surveillance sites should regularly communicate with providers within their jurisdiction via the telephone or a visit to the facility in order to determine if any births have occurred to women previously identified as HIV positive. In other cases, hospitals, obstetricians or pediatric case managers report directly to the local surveillance sites when they become aware of an HIV positive women's pregnancy or delivery. When an HIV positive woman's pregnancy is identified prior to delivery, the women's information should again be entered into a local database, and the women's prenatal care and HIV care should be tracked until her anticipated delivery date. **(Reports of known pregnant HIV infected women must be provided to DSHS on a monthly basis.)**

3.) Perinatal exposures may also be identified through review of laboratory results from rapid testing performed at delivery. Surveillance sites may learn about a pregnancy once the women has delivered through a laboratory report if the woman tests positive at delivery (i.e. via a rapid test) or by being notified by a health practitioner that a child has been born to an HIV positive woman.

4.) As of January 1, 2010, perinatal exposures may also be identified through laboratory reporting of negative Polymerase Chain Reaction (PCR) test results. Negative PCR test results for infants up to three years of age will now be reportable. (See Chapter 1-*Appendix A*: *Texas Reporting Rules*)

5.) And lastly, perinatal exposures may be identified through birth registry matches. A registry match between eHARS and the Vital Statistics birth registry is critical for ascertaining all possible mother/infant pairs so that data is representative of all HIV-infected pregnant women who were known to be HIV-infected during pregnancy. A registry match occurs when a woman's information in eHARS matches the maternal information on the infant's birth certificate. After conducting this match, HIV positive women who are identified to have given birth to a child that is not currently recorded in eHARS, will be forwarded to the respective surveillance site. DSHS will provide each eHARS site with a report for each potential perinatal exposure identified to have been born to an HIV positive woman. After investigation and within one month of receipt, all completed potential perinatal exposure reports should be returned to DSHS. The site will be required to complete a pediatric case report form for each confirmed perinatal exposure within 3 months of notification from DSHS.

2-5 Other Methods of Case Ascertainment

DSHS conducts yearly matching of the Texas birth defect registry with eHARS data. From this yearly matching, the Perinatal HIV epidemiologist will be able to identify children who were born with a birth defect and were recorded as being born to a woman receiving antiretrovirals. Children who are recorded in the Birth Defect Registry as being born to a woman receiving antiretrovirals and who are not recorded in the eHARS registry will be investigated to determine if in fact they were born to an HIV positive woman. In turn, children who are identified to have been born with a birth defect and whose information is not found in the birth defect registry will also be shared accordingly. The site will be required to complete a pediatric case report form within 3 months of notification from DSHS.

2-6 Follow-Up

The goal is for 85% of exposed infants born to have an HIV status determined (i.e., not be coded as indeterminate) 3 years after the birth. A child must be followed-up every six months until 18 months of age or until the child's HIV status has been determined, and, if they meet the HIV/AIDS case definition, will continue to be followed to determine their vital status. At a minimum of every six month interval, a pediatric case report form must be completed and eHARS must be updated with the new information. For indeterminate children, the follow-up form should indicate if a child is under active follow-up, child moved to another state, provider is out of state, child lost to follow-up, child died before status was determined, child less than 18 months of age or physician has designated the child as seroreverter despite the lack of necessary tests. **In cases where the physician has designated the child as a seroreverter despite the necessary tests, DSHS will contact the physician for further clarification.**

Chapter 3 Risk and COPHI

3-1 Risk Factor Ascertainment

A. Definitions

The following are risk-related terms as defined by the CDC:

1. Cases of public health importance (COPHI)

These are cases initially reported with a rare or unusual risk factor for HIV infection. Examples of these types of cases, which should be the first priority for follow-up, are occupational exposure, a human bite or tattoo, blood transfusion, or transplant recipient. See *Appendix A: Cases of Public Heath Importance (COPHI) and Protocol 776*.

2. Epidemiologic follow-up

This is the investigative process for obtaining additional information on a reported HIV/AIDS case.

3. No reported risk (factor) (NRR)

A case is classified as an NRR if it is reported without any risk factor information or with unconfirmed COPHI risk factor information.

4. No identified risk (factor) (NIR)

This is an NRR case for which an HIV risk factor cannot be identified or confirmed 1) although all available data sources have been reviewed or contacted; or 2) epidemiologic follow-up was either not initiated or not completed, but 12 months have elapsed since the date of the initial case report.

5. Risk factors

The collective term for the individual routes of exposure/transmission on which data are routinely collected for surveillance of HIV/AIDS cases. All risk factors listed on the case report form require a “yes,” “no,” or “unknown.” See *Appendix B: Risk Factors* for a list of risk factors.

6. Transmission category

The term used to summarize multiple risk factors (defined in *Appendix C: Transmission Categories*) that an individual may have had by selecting the one through which HIV was most likely to have been transmitted. The selection of the most likely route of transmission is based on a presumed hierarchical order of transmission that was developed in the early years of the AIDS epidemic. See *Appendix C: Transmission Categories* for a list of transmission categories.

B. Risk Factor Ascertainment

Surveillance staff should make efforts to obtain accurate and complete information on all risk factors when completing a CRF. Central Office expects to have an identified HIV risk factor for at least 85% of cases reported in a given year.

In order to improve completeness of risk factor information, all newly-reported HIV cases should have their medical record reviewed within 1 month of learning about the

case. Medical records should be reviewed thoroughly to ensure that any recorded risk factor information is captured. Depending on the facility of abstraction, risk factor information may be in any part of the medical record, so all sections of a medical record must be reviewed. Within three months of learning about a case, surveillance staff should also investigate other data sources (e.g. STD*MIS) or other facilities at which the case has received care in addition to the initial reporting facility when conducting epidemiologic follow-up of cases. These additional data sources should be prioritized based on where risk factors are most likely to found.
There are a number of sources from which risk factor information may be found, including:

- Medical record of testing provider
- Medical record of a treating provider
- Telephone call or visit to social service case manager
- STD*MIS
- Patient Interviews

Sites should continue to investigate cases with no reported risk until all reasonable sources of information have been reviewed. Sites should use every opportunity, such as telephone contact and facility visits, to continue to look for risk on cases.

To assist in the collection of risk factor information, Central Office will provide each surveillance site with a list cases missing an identified risk factor each month.

C. Complete Risk Factor Reporting
After reviewing a particular document source, the following risk factors must be completed for <u>all cases</u> (i.e. “yes,” “no,” or “unknown” must be checked). None of these risk factors should be left blank:

- Sex with male
- Sex with female
- Injected non-prescription drugs
- Received clotting factor for hemophilia / coagulation disorder

The following risk factors must have a response option checked if the <u>case is a male and “Sex with female” was marked “Yes"</u> or if the <u>case is female and “Sex with male” was marked “Yes”</u>:

- Heterosexual contact with intravenous/injection drug user
- Heterosexual contact with person with hemophilia / coagulation disorder
- Heterosexual contact with transfusion recipient with documented HIV infection
- Heterosexual contact with transplant recipient with documented HIV infection
- Heterosexual contact with person with AIDS or documented HIV infection, risk not specified

Additionally, <u>female cases with a “Yes” response to “Sex with male”</u> must also have a response marked for the following risk factor must have a completed response (i.e. “Yes,” “No,” or “Unknown”):

- Heterosexual contact with bisexual male

The following unusual risk factors should only be completed for cases where it is believed that the unusual risk factor was how the case may have acquired HIV. Selecting "Yes" to any of the following risk factors will initiate a COPHI investigation (see section 3-2)

- Received transfusion of blood / blood components (other than clotting factor)
- Received transplant of tissue / organs or artificial insemination
- Worked in a health care or clinical laboratory setting
- Other documented risk

Surveillance staff should collect multiple risk factors and not stop when a single risk factor has been identified.

3-2 Cases of Public Health Importance (COPHI)

Cases of public health importance are those cases with an unusual reported risk factor. Below is a summary of the types of risk factors that are considered to be cases of public health importance by the CDC. For more specific details on each of these risk factors refer to *Appendix A: Cases of Public Heath Importance (COPHI) and Protocol 776*.

A. NRR Risk Factors

Risk factors that occur in persons who are NRR (i.e. have no identified transmission category) that must be investigated include:

- Received transfusion of blood/blood components in the United States after March 1985
- Received clotting factor injection for hemophilia or another chronic coagulation disorder, and date of birth is after March 1985
- Received transplant of tissue/organs or artificial insemination
- Worked in a health care or clinical laboratory setting with possible exposure to human blood or other body fluids
- Women whose only sexual contact has been with another woman
- Other exposure to human blood or body fluids including but not limited to the following:
    - Household or other 'casual' contact
    - Patient exposure in a health care setting
    - Physical interaction where blood or body fluids were exchanged
    - Occupational exposure other than in the health care industry
    - Tattoo, piercing, other cosmetic exposures
    - Intentional self-inoculation or intentional inoculation by another person
    - Human bite
    - Other unusual circumstance (not previously identified as a risk factor)

B. Pediatric Risk Factors

Risk factors for pediatric cases that must be investigated regardless of whether the reported person has another risk factor include:

- Sexual contact with a male
- Sexual contact with a female

- Injected illicit or nonprescribed drugs
- Mother was known seronegative after the child's birth

C. HIV-2 and Variant Strain Surveillance

- Idiopathic CD4 lymphocytopenia
- HIV antibody negative or other laboratory test inconsistent with the clinical picture
- HIV-2
- Unusual strains including Group O

D. Unusual Manifestations

Unusual manifestations of clinical, laboratory, and geographic clusters of public health importance that relate to the HIV epidemic.

E. Investigation and Follow-up of COPHI Cases

Investigation and follow-up of COPHI cases are a CDC priority. If one of the aforementioned risk factors is identified for a case, this case will be flagged in eHARS as a potential COPHI case. All potential COPHI cases will be investigated to confirm the reported exposure. For all flagged COPHI cases the following steps will be taken.

1. The COPHI coordinator at Central Office will review all flagged cases at the time of report and contact each site regarding any potential COPHI case.
2. If the flagged case is determined <u>not to be</u> a potential COPHI case, then the risk factor will be corrected in eHARS and no further action will be taken. If the flagged case is determined <u>to be</u> a potential COPHI case, an investigation of the case will be initiated within 3 months of the date of initial case report or at the time of notification from the patient or provider, if not sooner. The CDC COPHI Coordinator will be contacted at this time.
3. The surveillance site will follow Protocol 776 (*Appendix A: Cases of Public Heath Importance (COPHI) and Protocol 776*) for case investigation. As part of the investigation the case will need to be interviewed if detailed risk factor information was not obtained through discussion with health care providers or review of medical records.
    a. If the surveillance staff are trained, they will perform the interview. If not, the interview will be assigned to a local DIS or a qualified Central Office staff member.
    b. Standard worksheets/questionnaires for COPHI are completed by the surveillance staff and sent to Central Office for review. Once patient identifiers have been removed, these forms will be sent to the CDC COPHI coordinator.
4. After completion of the investigation, if the risk factor is confirmed in consultation with the CDC, the case will be closed in eHARS with a final disposition. Cases will be closed after one year even if no information becomes available, but will be reopened to confirm risk factors at a later date.

COPHI instructions

Appendix X
Procedures for Investigations of HIV/AIDS Cases of Epidemiologic, Diagnostic, or Special Public Health Importance

August 2005

Table of Contents

I. BACKGROUND 3
1) Clusters of unusual clinical, laboratory or geographic occurrences that have potential public health Significance 3
2) Cases without detectable antibody response on standard testing (including blood donation screening) 3
3) Cases of HIV-2 and non-B subtypes in the United States 4
4) Possible unusual transmission circumstances where scientific evidence can confirm or refute the possibility of transmission, where possible 5
5) Non-perinatal exposure infections in children 5
6) Occupational exposures to HIV in health care and other settings 5
II. REPORTING REQUIREMENTS 5
III. CASE DEFINITIONS AND PROCEDURES 6
Seronegative HIV/AIDS Cases 6
Divergent strain Cases and HIV-2 Cases 6
Other Specific Cases of Public Health Importance 6
Female-to-female transmission: Exclusive female to female sex where the partner is known HIV positive and no other risk factors are identified 7
Sexual contact in pediatric cases 7
Needle use in pediatric cases 7
Pediatric cases where the mother was known to be HIV-negative at the time of the child's birth 7
Receipt of blood components that screened negative for HIV antibodies 7
Other suspected unusual circumstances 7
Occupational exposure 7
IV. SPECIMEN COLLECTION PROCEDURES 8
V. DATA MANAGEMENT 8
PROCEDURES FOR RECORDING/REPORTING RISK INFORMATION 8
DATA HANDLING, STORAGE AND DISPOSITION OF CASE RECORDS 9
VI. INVESTIGATION 9
VII. PROCESS AND PERFORMANCE STANDARDS 9
VIII. PROTECTION OF HUMAN RESEARCH PARTICIPANTS 10
RISKS AND BENEFITS 10
INFORMED CONSENT 10
CONFIDENTIALITY 10
IX. INVESTIGATORS AND CONTACT INFORMATION 11
X. REFERENCES 14
APPENDIX A 16
GENERAL GUIDELINES FOR INVESTIGATION OF CASES OF SUSPECTED UNUSUAL TRANSMISSION 16
APPENDIX B 19
POST-SCREENING TRANSFUSION FOLLOW-UP INVESTIGATIONS 19
APPENDIX C 20
TRANSPLANT INVESTIGATIONS 20
APPENDIX D 21
INVESTIGATION OF SEXUAL TRANSMISSION IN CHILDREN 21
INFORMATION TO COLLECT IN A PEDIATRIC CASE INVESTIGATION 22
APPENDIX E. 25
INVESTIGATION OF SUSPECTED OCCUPATIONAL EXPOSURES 25
APPENDIX F 26
HIV-2 CASE DEFINITION[1] 26

I. BACKGROUND

Since 1981, CDC has systematically collected data regarding probable mode of HIV risk exposures. These data provide the largest population-based collection of HIV risk factor/exposure data available in the U.S. and are used to: 1) monitor trends in transmission, 2) identify new or unusual transmission circumstances, 3) identify behavioral risks to target risk reduction interventions and allocate prevention resources, 4) provide evidence to support the lack of transmission in certain settings or under certain circumstances, and 5) provide data for projection analysis. The need to continue to collect high quality risk factor information remains a priority in order to adequately reflect the current epidemic.

Cases of public health importance are those cases where either the risk factor reported is unusual and should be brought to the attention of CDC or where other circumstances exist, such as unusual strains of HIV, that necessitate investigation, intervention or communication with CDC. These include (but are not limited to):

1) Clusters of unusual clinical, laboratory or geographic occurrences that have potential public health significance

People who become infected with HIV may have multiple high risk exposures to other infectious agents. The HIV/AIDS surveillance system may identify and investigate unusual manifestations of clinical, laboratory, and geographic clusters of public health importance that relate to the HIV epidemic. These unusual occurrences may include, but are not limited to: clusters of co-infections with tuberculosis, hepatitis, or other sexually transmitted diseases (STD) and HIV; adverse outcomes of long-term antiretroviral therapy; changes in the ability of licensed tests to detect HIV antibody; threats to the blood supply due to defective test kits; and resistant strains of an STD in an immunosuppressed person.

2) Cases without detectable antibody response on standard testing (including blood donation screening)

Cases or suspected cases of HIV infection without detectable antibody response are probably rare events, but should be considered cases of highest public health priority because they could be associated with screened-negative HIV-infected blood or plasma donations, tissue or organ transplants, or because they could represent a newly emerging agent factor with implications for HIV diagnostics.

Clinical diagnosis of HIV-1 infection and screening of blood donations relies on detection of antibodies to HIV-1 in the serum or plasma of patients. Initial screening is done using a licensed enzyme immunoassay (EIA) screening kit; for specimens with reactive EIA results, HIV infection is confirmed using a Western blot or IFA test.

There may be several reasons for negative HIV screening results in patients who are HIV-infected. The most well recognized of these is “window period” collection (i.e. collection of a blood specimen during the time between infection with HIV and the advent of a detectable antibody response). In 2005, this window period is generally between 7–22 days following exposure, depending on the specific EIA reagents or other screening tests used.[1,2] Since May 1996, screening of blood donations has also included testing for the presence of HIV-1 p24 antigen[3]. In October 2004 the FDA approved Nucleic Acid testing (NAT)[4] for screening. Since NAT has been found to detect HIV earlier in the window period than p24 antigen, many blood centers are using NAT and eliminating the p24 antigen test.

Other possible causes of negative antibody screening results in HIV-infected patients include infection with non group M subtype B HIV-1,[5] conversion from antibody seropositive to antibody seronegative status (seroreversion), and laboratory or attributional errors. Although HIV-infected patients in late

stages of disease may have decreasing antibody titers to some HIV antigens, with current, highly sensitive antibody EIA kits, true seroreversion is very rare.[5]

Several case reports have described patients with recognized HIV infection and persistently seronegative antibody screening results. In some of these cases, the clinical progression of HIV disease has been very rapid,[6] leading to the hypothesis that some patients may fail to develop antibodies following primary HIV infection, and that this lack of antibodies allows rapid progression of disease. In two cases,[7,8] HIV-infected partners who were infected with the same viral strain as the seronegative partner had detectable antibody responses; this supports the hypothesis that lack of detectable antibody response is a result of a defect in the host immune system (a host factor), rather than of a viral characteristic (agent factor).

3) Cases of HIV-2 and non-B subtypes in the United States

Comprehensive surveillance of the HIV/AIDS epidemic includes surveillance of other variant strains that may not react to standard FDA approved HIV-1 tests. HIV type 1 (HIV-1) and type 2 (HIV-2) both cause AIDS. Efforts to prevent transmission of HIV-1, particularly through the blood supply, led to the development of diagnostic tests for HIV-1 antibodies, in 1985. Because HIV-2 infections are not always detected by HIV-1 tests, antibody tests for HIV-2 infections were developed. The FDA licensed an enzyme immunoassay (EIA) test kit for HIV-2 on April 25, 1990. Since 1990, each revision of the HIV/AIDS surveillance case report form has included data collection fields for HIV-2 test results. Beginning June 1992, the FDA recommended that all donated blood, blood products, and plasma be screened for HIV type 2 (HIV-2). Although considerable serologic cross-reaction occurs between HIV-1 and HIV-2, HIV-2 infection may not be diagnosed when screening is done exclusively with HIV-1 tests.

Numerous HIV strain types have been identified, based primarily on variations in the env genes, which code for the viral envelope proteins. The different strain types have been classified as HIV 1 group M (subtypes A J), HIV 1 group N, and group O, and HIV 2, according to the degree of their relatedness to each other as determined by phylogenetic analysis. Although subtype B isolates were first identified in North America and are believed to represent the majority of isolates in North America and Western Europe, the other subtypes have varying geographic distributions throughout the world. HIV 2 strains, primarily found in Western Africa, have not been as well characterized.

HIV 1 group O strains,[9] are a highly divergent group of HIV not reliably detected by routine enzyme immunoassay (EIA) testing methods.[10] The group O strains are primarily found in Central Africa, particularly in Cameroon (estimated to account for less than 10% of HIV infection in Cameroon). Although uncommon, group O strains have begun to appear outside of Central Africa. In the U.S., the first case of HIV 1 group O infection was identified in a woman originally from West Africa in April 1996,[11] and more recently, a second case was confirmed.[12] As of June, 2005 there are two licensed EIAs that included testing for Group O. Group O infections usually test positive on HIV-1 western blots although they may have diminished envelope reactivity or might register an indeterminate result.

Less is known concerning detection of HIV 1 group M, non B subtypes by currently licensed EIA kits to detect antibodies to HIV 1. Recent data indicate that, among HIV and AIDS cases identified through national HIV/AIDS surveillance, for some communities a significant proportion of HIV 1 infections may be with group M, non B subtypes of HIV-1.[13] Individuals who are group O or HIV-2 infected and receive negative HIV test results may represent unrecognized infections or have inaccurate results when tested using viral load testing,[15] and, based on in vitro data, may have decreased response to therapy with certain routinely used antiretroviral medications.[16] Therefore, CDC will continue to work with state and local health departments to investigate potential cases of HIV-2 and to institute mechanisms for identifying and monitoring infections with group O and other unusual HIV strains.

4) Possible unusual transmission circumstances where scientific evidence can confirm or refute the possibility of transmission, where possible
Examples of unusual transmission circumstances include (but are not limited to): transplants (including artificial insemination), female-to-female transmission, transmission of HIV from a health care worker to a patient, household transmissions, and other suspected unusual circumstances (e.g. tattoo, human bite, intentional self-inoculation). Several examples of these are cited in the references.[17–19]

5) Non-perinatal exposure infections in children
These include suspected sexual contact in pediatric cases, suspected non-prescription needle use and cases where the mother was known HIV negative at the time of the child's birth.

6) Occupational exposures to HIV in health care and other settings
Health care workers reported without another known risk factor are a high priority for follow-up risk investigations. These cases are handled by the Prevention and Evaluation Branch, Division of Healthcare Quality Promotion at NCID. Transmission of HIV from a health care worker to a patient is also a public health priority and is handled by the Division of HIV/AIDS Prevention.
Data on occupational exposure to HIV are useful in evaluating the extent of HIV transmission in various health care and public safety settings and has practical value to CDC, NIOSH, OSHA, and health professional organizations in formulating more effective prevention strategies in these areas.[20] These data are also useful to manufacturers of medical devices and personal protective equipment in designing safer products and to occupational groups for education and review of recommended infection control practices.

II. REPORTING REQUIREMENTS

All project areas receiving HIV/AIDS surveillance funding are expected to report such cases as part of their core surveillance requirement (50 states, any separately funded cities, the District of Columbia and U.S. Trusts and Territories). The follow-up of such cases by State health department and CDC staff will be coordinated and prioritized within each organization. Communication between the organizations is essential. A staff person at both the state/local level and at CDC should be identified and function as the coordinator for follow-up investigations.

State and local health departments should inform all care providers who report HIV/AIDS cases to be alert to possible unusual HIV transmission circumstances and to call the State health department when such a possibility exists. The State health department in turn should call CDC to inform us that an investigation is proceeding.

Any person who meets a case definition as outlined in Section III is eligible for investigation through medical record review and discussion with health care providers. All persons, except prisoners and persons less than 18 years of age are eligible for interview and blood draw. Children under 18 years of age can be eligible if parent or guardian signs appropriate consent form.

Epidemiologic investigation of cases infected with divergent HIV strains will be conducted on a case-by-case basis, based on the public health importance of the strain in question and the laboratory characteristics of the infection.

Participants may choose to discontinue voluntary participation in an investigation at any time. If a participant decides that they no longer want to participate in the investigation or allow further testing of laboratory specimens, they will contact the HIV/AIDS surveillance staff at the State health department who will then contact all appropriate persons to inform them of the decision to discontinue the investigation and/or laboratory analysis.

III. CASE DEFINITIONS AND PROCEDURES

Cases cannot be called "confirmed" without CDC review of available documentation and laboratory results. It is better to contact CDC prior to beginning any investigation that will require additional effort beyond that of routine surveillance case follow-up. We anticipate that the majority of cases will be closed for a variety of reasons: another more common risk factor is identified, persons refuse interview and/or blood draw, persons are lost to follow-up, or, while the claim may be legitimate, insufficient documentation of the event makes confirmation impossible. Timely reporting and follow-up of cases while documentation and memory of events by affected persons is fairly recent can make the difference between a confirmed case and one closed due to insufficient information.

Case definitions are defined on an as-needed basis when a case or group of cases, identified through routine HIV/AIDS surveillance reporting, indicates the need for additional follow-up investigations to address questions having potential public health implications. Therefore, some categories listed below may not have a standard definition.

1. Seronegative HIV/AIDS Cases
   a. Adults and adolescents (≥13 years of age) are seronegative HIV/AIDS cases if they have infection with HIV-1, documented by positive DNA or RNA-PCR or viral culture drawn from two specimens on different dates; and with at least two negative antibody screening test results from independent laboratories on two specimens collected on different dates.
2. Divergent strain Cases and HIV-2 Cases
   a. Adults and adolescents (≥13 years of age) are divergent strain cases if they show laboratory evidence of humoral response to HIV-2 or non-subtype B antigens, or if sequence analysis of clinical isolates give results indicative of infection with a divergent HIV strain.
   b. This can also include cases that are antibody positive but with persistently undetectable viral load tests without therapy
   c. See Appendix F for further information on HIV-2 testing and the case definition.

3. For cases listed in 1) and 2), contact the CDC COPHI coordinator to arrange possible shipment of specimens to CDC for laboratory testing and HIV-2 or variant strain sub-typing. Some demographic information will be requested including: Sex, Race/ethnicity, date of birth, country of origin, CD4 T lymphocyte counts and any other previous test results relating to HIV.

4. Other Specific Cases of Public Health Importance
   a. Transplants
      i) Documented: receipt of a transplanted organ that screened negative for HIV-antibody in a person for whom no other risk factor was identified and for whom an HIV seropositive donor was identified.
   b. Artificial insemination:
      i) Documented: women with a seropositive sperm donor and no other risk for HIV infection
      ii) Suspected: 1) women with a history of artificial insemination for whom no other risk has been identified, and for whom a seropositive donor has not been identified, and 2) women with a history of artificial insemination who have other risk factors for HIV, as well as an identified seropositive donor.

c. Female-to-female transmission: Exclusive female to female sex where the partner is known HIV positive and no other risk factors are identified
d. Sexual contact in pediatric cases
   i) Documented: The child must have
      (1) A diagnosis of HIV/AIDS,
      (2) A diagnosis of sexual abuse based on physical examination or physician diagnosis; child, care-giver, or perpetrator disclosure; previous or concurrent non-congenital sexually transmitted disease; prosecution of perpetrator; or pregnancy, and
      (3) Documentation of an HIV-infected or high-risk perpetrator. A perpetrator is considered to be at high risk if he engages in male-to-male sexual contact or if he/she is an injection drug user or has hemophilia or other coagulation disorder.
   ii) Suspected: The child must have
      (1) Confirmed HIV infection or AIDS,
      (2) A diagnosis of sexual abuse, and
      (3) No other risk factor for HIV.
         (i) These cases are suspected and not confirmed because the following information is unavailable: the identity, HIV serostatus, or HIV risk of the perpetrator.
e. Needle use in pediatric cases.
f. Pediatric cases where the mother was known to be HIV-negative at the time of the child's birth.
g. Receipt of blood components that screened negative for HIV antibodies (after 3/85) and p24 antigen (3/96), by a person for whom no other behavioral risk factors were reported and for whom a seropositive blood donor has been identified
   i) Documented: Receipt of blood or blood products that screened negative for HIV antibodies (after 3/1985) and p24 antigen (after 3/15/1996), in a person for whom no other behavioral risk factor information was reported or identified and for whom a seropositive blood donor was identified.
   ii) Persons reported whose only risk factor for HIV is the receipt of a blood transfusion after March, 1985 are investigated to determine the likelihood of the transfusion as the mode of transmission. Cases that cannot be re-classified to another risk or for whom documentation of a post-screening transfusion risk is unavailable, are closed as incomplete, either because the serostatus of all donors is not known or because receipt of the transfusion cannot be verified (e.g., transfusions received in a foreign country) and therefore no look-back study can be done to determine the serostatus of the donors.
h. Other suspected unusual circumstances (e.g. household transmission, tattoo, bite, intentional self-inoculation).

For cases listed in 3 a – h, contact the CDC COPHI coordinator once you have confirmed with the provider that one of the risk factors listed above is being considered the primary mode of exposure. For adults/adolescents complete the demographics and NIR modules of the questionnaires. When the purported source of infection is known, specimens may be requested to confirm or refute the hypothesis of infection from one individual to the other.

i. Occupational exposure
   i) Documented: Evidence of HIV seroconversion in temporal association with an occupational exposure and no other known exposure to HIV during the same time period. Seroconversion is defined as a serum specimen that has been negative for HIV antibody up to one year before or one month after the occupational exposure. Also included in this category are persons infected with HIV strains that are shown to be related to the occupational source through DNA sequencing techniques. A health care worker (HCW)with a history of high-risk behaviors for HIV infection is classified as having documented occupationally acquired

infection if the health department's epidemiologic investigation concluded that an occupational contact was the only exposure to HIV during the period when seroconversion occurred, or if the viruses of the HCW and the occupational source of exposure were shown to be related through DNA sequencing.

ii) Possible: Person who reports no behavioral risk for HIV infection or transfusion of blood or blood products before March, 1985, but reports past percutaneous or mucocutaneous occupational exposures to blood or body fluids or to HIV-containing laboratory specimens. Seroconversion as a result of an occupational exposure cannot be established, and the time and source of HIV infection for that HCW cannot be documented.

Occupational exposures involving infection of a health care worker from an HIV-infected source patient are the primary responsibility of the Division of Health Quality promotion (DHQP) (see contact information in Section IX of this document). However, an investigation of a health care worker exposure usually begins with an assessment of other possible risk factors for HIV necessitating involvement of the COPHI coordinator. Therefore, investigations are usually handled jointly. For HIV exposed health care workers who received post-exposure prophylaxis and subsequently tested positive for HIV, please notify DHQP for possible entry in the PEP Failure protocol.

Occupational exposures involving occupational exposures not in a health care setting or health care settings where the worker has potentially infected a patient should be brought to the attention of the COPHI coordinator.

IV. SPECIMEN COLLECTION PROCEDURES

For some cases, blood specimens may be collected for laboratory studies and future testing. Blood specimens will be collected if the epidemiologic investigation determines there is a public health need to do testing beyond that which has already been conducted and documented. Personnel from the State health department and from the HIV Incidence and Case Surveillance Branch (HICSB) and the Laboratory Branch, DHAP, will be consulted to determine if there is a public health need for the collection of specimens. **HICSB staff at CDC should be consulted before obtaining blood specimens.**

Laboratory test results will be reported to the State health department, which in turn will contact the participant or their provider to inform them of the results.

V. DATA MANAGEMENT PROCEDURES FOR RECORDING/REPORTING RISK INFORMATION

Risk factor information is routinely collected by the State/local health departments using the Adult and Pediatric HIV/AIDS Confidential Case Report Forms. Risk factor information is entered into the computerized HIV/AIDS surveillance database at the State and sent to the CDC monthly or bi-monthly for upload into the national database.

If detailed risk factor information is not obtained through discussion with health care providers or review of medical records and the case is a priority for follow-up, the person with HIV/AIDS (PWHA) will be asked to participate in an interview. Approaching an individual to discuss their risk of HIV infection should be based on the recommendations of the health care providers involved and on the experience of the health department staff.

A proxy interview will only be considered in the very rare event that 1) the case is a high priority for investigation, 2) the PWHA is dead or unable to participate in an interview because of their mental or physical health condition, and 3) an appropriate proxy can be identified. An appropriate proxy would be

someone who knows the PWHA, knows their infection status, and would probably know the kinds for information asked on the questionnaire.

Standard worksheets/questionnaires for COPHI are completed by State/local health department personnel and may be sent to the CDC coordinator for review once patient identifiers have been removed for confidentiality. Further discussion of confidentiality of forms is contained in the Section VIII of this document. Contact the CDC COPHI coordinator if there are questions about which form(s) to use.
There are six worksheets currently available as electronic documents:

1) Module A - Demographics
2) Module B - No Identified Risk
3) Module C - Occupational exposure
4) Module D - HIV-2 and variant strains
5) Module E - Female to female transmission
6) Pediatric sexual abuse assessment

DATA HANDLING, STORAGE AND DISPOSITION OF CASE RECORDS

Once a case has been closed, the questionnaires and all accompanying documentation are filed in a secure storage area at CDC by State and State number and without patient identifiers. Records are eventually archived to off-site storage.

VI. INVESTIGATION CLOSURE

The following guidelines will be used for closing investigations:

1) If other risk information becomes available or the case is confirmed as a COPHI, the HIV/AIDS Reporting System software will be updated with the risk information.
2) If the case is interviewed, the appropriate modules of the CDC standardized questionnaire should be completed and forwarded to CDC.
3) If no risk could be confirmed and no interview was conducted:
    - Cases open for at least one year will be reviewed for possible closure. If no further follow-up is anticipated and information is deemed unavailable, the case will be closed.
    - The case will be left open if there is a specific reason to do so (e.g., health department believes patient will discuss risk at later time or high priority status). Cases left open will be reevaluated for closure every 6 months until closed.
    - Follow-up on a case will be completed and the case closed within a reasonable amount of time following receipt by the State/city health department of death notification unless there is a specific reason to keep the case open
    - Cases may be re-opened at any time that new information becomes available.

VII. PROCESS AND PERFORMANCE STANDARDS

There is no minimum performance standard. All cases of public health importance should be investigated to the extent possible and closed.

Any case with a risk factor or variant strain (as described in Sections I and III) that is reported to the health department should be identified at data entry and referred to the appropriate staff member. The staff member should contact the provider or reporter to ascertain whether the case requires investigation. If it is determined that the case has another more common risk factor and that this is not a COPHI, the HIV/AIDS Reporting System software should reflect this change. Reports should be run every six months at a minimum to identify cases requiring investigation.

A yearly report of COPHI and the final disposition of each case should be run using the HIV/AIDS Reporting System software.

VIII. PROTECTION OF HUMAN RESEARCH PARTICIPANTS

RISKS AND BENEFITS

The risk to participants of these investigations is minimal. Participants who consent to an interview may experience some degree of emotional anxiety or distress when asked personal questions of a highly sensitive nature. Also, participants who consent to a blood draw may feel a “pinch” associated with having a venipuncture. They may also experience some bruising and or soreness at the site of the needle stick. In rare instances, they may experience fainting associated with the procedure.

The participant could benefit from blood testing performed as part of the study. Verification of HIV infection status and the results of subtyping of the HIV virus may have direct application to the clinical management of the patient. Both the interview and blood draw component of the investigation will help CDC and the health care community better understand the risks of HIV and how better to prevent its transmission as well as allowing for a more complete epidemiologic and laboratory profile of HIV-infected patients without detectible antibody responses. Both components will also allow for the important collection of standardized data on the occurrence of HIV-2 and non-B subtypes of HIV-1 in the United States.

INFORMED CONSENT

Written informed consent will be obtained from all persons with HIV/AIDS (and/or their proxies) prior to an interview or blood draw. **The CDC approved consent form is now required to be used to obtain participant's consent in any cases where CDC will be performing laboratory tests.** The person conducting the interview or blood draw (usually a State or local health department staff person) will discuss the consent with the participant, explaining how the information gathered will be used and answering any questions the participant may have. The investigator will review the consent form with the participant and answer any questions that may arise. The participant will be asked to sign the consent form. **These consent forms will be kept by the State, local, or territorial health department and neither the original nor any copy will be sent to CDC. A copy of the consent form will be given to the participant.**

State health departments may also elect to use their own departmental consent forms. While this is allowed, the CDC consent form must also be used for any cases where information and/or laboratory specimens are sent to CDC for review.

CONFIDENTIALITY

No CDC HIV/AIDS surveillance information that could be used to identify individuals, either directly or indirectly, will be made available to anyone for non-public health purposes. In particular, such information will not be disclosed to the public, parties involved in civil, criminal, or administrative litigation (within the limits of the law), or non-health agencies of the federal, state, or local government. Results of these investigations, without any personally identifying information, may be described in a written document explaining the outcome of the investigation.

Information on these individuals that is provided to CDC should be identified by the health department state number. The consent form and any personal identifying information contained on the first page of the interview form should be retained by the State, local, or territorial health department. All personal identifiers including name, address and social security number should be removed from the body of the interview form and any other documentation (such as copies of medical records) before being mailed to CDC. All information collected is covered under an Assurance of Confidentiality at CDC. The

Assurance of Confidentiality is guaranteed under Sections 306 and 308(d) of the Public Health Service Act (42 U.S.C. 242K and 242m(d)). Persons involved in these investigations should maximize their efforts to protect this confidentiality.

Surveillance information reported to the CDC will be used without identifiers for statistical and analytic summaries in which no individual can be identified. When necessary for confirming surveillance information or in the interest of public health and disease prevention, the CDC may confirm information contained in case reports or may notify other medical personnel or health officials of such information; in each instance, only the minimum information necessary will be disclosed.

IX. INVESTIGATORS AND CONTACT INFORMATION

Centers for Disease Control and Prevention (CDC), National Center for HIV, STD, and TB Prevention (NCHSTP), Division of HIV/AIDS Prevention, Surveillance Branch:

Adelisa Panlilio, MD, MPH, Co-investigator (Healthcare worker exposures)
Kate Glynn, DVM, MPVM, Co-investigator
Lata Kumar, Coordinator for investigations of HIV/AIDS Cases of epidemiologic, diagnostic, or special public health importance

Investigations and interviews will be conducted by State, local, and/or CDC personnel responsible for HIV/AIDS surveillance activities as deemed appropriate by State, local, and CDC staff. Laboratory analyses will be conducted by CDC staff in the National Center for HIV, STD and TB Prevention, Division of HIV/AIDS Prevention Laboratory Branch. Investigations of potential health care worker occupational exposures will be handled by the Division of Health Quality Promotion, National Center for Infectious Diseases.

Although several people may be involved in any one investigation, one individual in each State health department and one individual at CDC will serve as primary coordinator and contact for any investigation being conducted.

CDC Contact Persons

All questions about investigation of cases of suspected unusual transmission (including possible postscreening transfusion and organ/tissue transplant risks) will be directed to:

HICSB COPHI Coordinator
As of 1/2006: Lata Kumar, MPH
(404) 639-2050
Centers for Disease Control and Prevention
NCHSTP/DHAP
HIV Case and Incidence Surveillance Branch
MS E-47
1600 Clifton Road, NE
Atlanta, GA 30333
LKumar@cdc.gov

For questions about other investigations of public health importance, initial contact can be made to the person listed above. Depending on the circumstances of the investigation, the most appropriate Surveillance Branch staff person will be designated as the primary contact at CDC.

Questions about investigations of persons with potential health care worker occupational exposures will be directed to:

Adelisa Panlilio, MD, MPH
Centers for Disease Control and Prevention
NCID/Division of Health Quality Promotion
MS E-68
1600 Clifton Road, NE
Atlanta, GA 30333
(404) 498-1265
APanlilio@cdc.gov

There is also a Needlestick Resource Center: (404) 498-1250 or (toll free) (800) 893-0485
For post-exposure prophylaxis failure contact the PEP failure hotline: (888) 448-4911

Contact for questions on divergent HIV strains, HIV-2 and testing methodologies is:

Bernie Branson, MD
Centers for Disease Control and Prevention
Associate Director for Laboratory Diagnostics
MS D-21
1600 Clifton Road, NE
Atlanta, GA 30333
(404) 639-6166
BBranson@cdc.gov

Blood transfusion safety involving HIV:

Matthew Kuehnert, MD, MPH
Associate Director of Blood Safety
Division of Viral and Rickettsial Diseases, NCID
CDC

1600 Clifton Road, NE
MS A-30
Atlanta, GA 30333
(404) 639-4350
MKuehnert@cdc.gov

Laboratory contact for cases requiring genotypic analysis:

Marcia Kalish
Associate Chief For Science
DHAP Laboratory Branch
CDC
1600 Clifton Road, NE
MS G-19
Atlanta, GA 30333
(404) 639-3957
MKalish@cdc.gov

Laboratory contact for cases requiring testing for HIV-2 or divergent strains:

Michele Owen
DHAP Laboratory Branch
CDC
1600 Clifton Road, NE
MS A-25
Atlanta, GA 30333
(404) 639-1046
MOwen@cdc.gov

CDC Surveillance staff should be notified prior to the shipment of any laboratory specimens to CDC. The address for shipment of specimens is:

CDC Serum Bank Branch
602 Webb Gin House Road
Lawrenceville, GA 30245-5427
Phone: (770) 339-5917
FAX: (770) 339-5915
SBartley@cdc.gov
DHemmerlein@cdc.gov

Primary contacts: Suzette Bartley and Dollene Hemmerlein

X. REFERENCES

1. Busch MP, Kleinman SH. Nucleic acid amplification testing of blood donors for transfusion-transmitted infectious diseases. Transfusion 2000; 40: 143–59.

2. Tabor E, Epstein JS. NAT screening of blood and plasma donations: evolution of technology and regulatory policy. Transfusion 2002; 42: 1230–7.

3. Centers for Disease Control and Prevention. U.S. Public Health Service guidelines for testing and counseling blood and plasma donors for human immunodeficiency virus type 1 antigen. MMWR. 1996; 45 (RR-2): 1–9.

4. Food and Drug Administration. Center for Biologics Evaluation and Research. Guidance for Industry. Use of nucleic acid tests on pooled and individual samples from donors of whole blood and blood components (including source plasma and source leukocytes) to adequately and appropriately reduce the risk of transmission of HIV-1 and HCV. October 2004.

5. Roy MJ, Damato JJ, Burke DS. Absence of true seroreversion of HIV-1 antibody in seroreactive individuals. JAMA 1993; 269(22): 2876–2879.

6. Martin-Rico P, Pedersen C, Skinhej C, et al. Rapid development of AIDS in an HIV-1 antibodynegative homosexual man. [Letter] AIDS 1995; 9(1): 95–96.

7. Reimer L, Mattice S, Schable C, et al. Absence of detectable antibody in a patient infected with human immunodeficiency virus. Clin Infec Dis 1997; 25: 98–100.

8. Michael NL, Brown AE, Voigt RF, et al. Rapid disease progression without seroconversion following primary human immunodeficiency virus type 1 infection—evidence for highly susceptible human hosts. J Infect Dis 1997; 175 (6): 1352–9.

9. De Leys R, Vanderborght B, Haesevelde MV, et al. Isolation and partial characterization of an unusual human immunodeficiency retrovirus from two persons of west-central Africa origin. J Virol. 1990; 64 (3): 1207–1216.

10. Schable C, Zekeng L, Pau CP, et al. Sensitivity of United States HIV antibody tests for detection of HIV-1 group O infections. Lancet. 1994; 344: 1333–1334.

11. Rayfield MA, Sullivan P, Bandea CI, et al. HIV-1 group O virus identified for the first time in the United States. Emerging Infect Dis. 1996; 2(3): 209–212.

12. Sullivan PS, Do AN, Robbins K, et al. Surveillance for variant strains of HIV: subtype G and group O HIV-1. JAMA. 1997; 278(4): 292.

13. Sullivan PS, Do AN, Ellenberger D, et al. Human immunodeficiency virus (HIV) sub-type surveillance of Africa-born persons at risk for group O and group N HIV infections in the United States. JID 2000; 181: 463–469.

14. Dunne AL, Crowe SM. Comparison of branched DNA and reverse transcriptase polymerase chain reaction for quantifying six different HIV-1 subtypes in plasma. AIDS. 1997; 11 (1): 126–127.

15. Schutten M, von der Ende ME, Antiretroviral therapy in patients with dual infection with human imunodeficiency virus types 1 and 2. NEJM 2000; 342 (23): 1758–60

16. Simonds RJ, Holmberg SD, Hurwitz RL, et al. Transmission of human immunodeficiency virus type 1 from a seronegative organ and tissue donor. NEJM 1992; 326: 726–32.

17. Centers for Disease Control and Prevention. HIV transmission between two adolescent brothers with hemophilia. MMWR. 1992; 42 (49): 948–951.

18. Centers for Disease Control and Prevention. HIV infection in two brothers receiving intravenous therapy for hemophilia. MMWR. 1992; 41 (14): 228–231.

19. Fitzgibbon JE, Gaur S, Frenkel LD, et al. Transmission from one child to another of human immunodeficiency virus type 1 with a zidovudine-resistance mutation. NEJM 1993; 329 (25): 1835–1841.

20. Centers for Disease Control and Prevention. Update: investigations of persons treated by HIVinfected health-care workers—United States. MMWR. 1993; 42 (17): 329–331, 337.

APPENDIX A
GENERAL GUIDELINES FOR INVESTIGATION OF CASES OF SUSPECTED UNUSUAL TRANSMISSION

Objective

The primary focus of an investigation is to determine whether or not the person with HIV/AIDS has contracted HIV through a circumstance not previously documented in the scientific literature and/or through circumstances where the safety of the public might be in jeopardy if an investigation (and appropriate follow-up) were not done.

Resources

1. Health care providers (including):
   - Infectious disease physicians
   - Infection control practitioners
   - Nurses
   - Primary physicians
   - Social workers

2. Medical records:
   - Inpatient records (acute care hospital)
   - Outpatient clinic records
   - Physician's office records

3. Other records (including but not limited to):
   - Sexually transmitted disease (STD) records
   - Hepatitis B registry

5. Patient interview

Approach

Keep an open mind when investigating a case. Often when a provider calls the health department to report a case, the patient may already have some theory as to how he/she may have contracted HIV and this information will be passed on to health department officials. To obtain a complete picture collect the following information (go back as far as the last negative HIV test or the last 10 years up to the time of HIV diagnosis):

1) Demographic

- Age
- Country of birth—if not from the U.S. how long has the person been in the U.S.? Any potential
- exposures in the home country?
- Date of birth
- Gender
- Level of education
- Marital status—how long married, HIV status of spouse,
- Any close relatives with HIV
- Race

2) Drug Use History

- Skin popping of drugs
- Use of crack, cocaine, heroin, crank, speed, barbiturates, PCP or any other drug
- Use of any drug intramuscularly or intravenously
- Visits to a drug 'shooting gallery'
- Visits to a 'crack house' or sex in a 'crack house'

3) Medical History—Any of the following: [collect dates of procedures, physician's name, facility where procedure performed]

- Activities involving contact with needles, knives, blood
- Acupuncture or other alternative medical therapy
- Artificial insemination
- Dental work
- Hepatitis, hepatitis vaccine, hepatitis immune globulin
- History of any sexually transmitted diseases
- Hospitalizations
- Injections by non-medical care personnel
- Medical conditions requiring frequent injections (e.g. diabetes, steroids, etc.)
- Organ or tissue transplants
- Receipt of blood or blood products
- Surgeries

4) Military History (in the last 10 years or before the diagnosis of HIV infection)

- Drug use while in the military
- Sexual contacts while in the military (if contacts occurred outside the U.S., collect details regarding country, date, gender and risk of partner, etc.)

5) Occupational history

- Dates of jobs
- Employment in a health care facility, clinical laboratory or as a public safety worker (policeman, fireman, emergency medical technician)
- Location of jobs
- Type of jobs

6) Prison/Jail History

- Drug use while incarcerated
- Sexual contacts while incarcerated
- Other possible exposures (receipt of tattoos, bloody brawls, etc)

7) Sexual History

- Age at first sexual intercourse
- Any sex partners with HIV or at high risk for HIV (heterosexual and same-sex partners)
    - Person with HIV/AIDS

    - Man who had sex with another man
    - Person who has used injection drugs
    - Person who has received blood or blood products
    - Person who has had a transplant or received artificial insemination
    - Person born outside the U.S. in a country where heterosexual transmission of HIV predominates
    - Person who has ever accepted money or drugs for sex (prostitute, commercial sex worker)
- Exchange of sex for money or drugs
- History of rape
- Number of opposite and same sex partners
- Kinds of sex participated in
    - Anal
    - Oral
    - Vaginal
- Whether a person's sex partners have had sex with a person in a high-risk category as listed above

8) Shared Residence

- Shared residence with a person with HIV infection or known to have AIDS
- Home health care administration to a person with HIV or AIDS
- Shared residence with a person at high risk for HIV infection as listed in 7).

9) Travel History

Travel outside of the U.S. and receipt of any medical care, injections, or sexual contacts while outside the country

APPENDIX B

POST-SCREENING TRANSFUSION FOLLOW-UP INVESTIGATIONS

Persons reported with HIV/AIDS whose only risk of HIV infection is receipt of a blood or blood product after March, 1985 should be investigated to: identify other risk factors for HIV, initiate blood center lookback studies if appropriate, and to confirm and document the transfusion risk.

Medical record reviews will often determine that persons reported with a post-screening transfusion risk received the transfusion at a date earlier than that initially reported, or that the date of the transfusion was incorrect. When the initial date reported is correct and it is after March, 1985, check with the blood center to determine exactly when antibody testing (screening) of the blood supply at that center was begun. Although the antibody test was licensed in early March 1985, some blood centers did not begin using the test until several months later.

If it is determined that the case only received screened blood, investigate for other HIV infection risks using the standard NIR procedures. If extensive follow-up fails to yield other risk factors, then the blood donors should be evaluated for HIV infection. The unit numbers for each of the blood components should be contained in the medical records. In some cases, the facility where the transfusion took place will contact the appropriate blood center, but in most cases, the health department will contact the blood center directly. The blood center conducts a look-back study to determine if any of the donors were found to be HIV positive during a subsequent donation. An attempt is made to contact those donors who have not returned for subsequent donation. These persons are asked to consent to HIV testing.

Regulations pertaining to the Social Security Administration's (SSA's) Blood Donor Locator Service were published in the Federal Register on December 24, 1991. Based on these regulations, if a State agency or authorized blood donation facility have been unable to locate blood donors who may be infected with HIV, the SSA will furnish to participating State agencies, at their request, the donor's last known personal mailing address.

CDC assistance with these investigations may be requested and should be requested in the case of interstate circumstances. If requested, an epidemiologist from the HIV Incidence and Case Surveillance Branch will be assigned to assist with the investigation. Because cases involving documented post-screening transfusions are tracked and reported, a written summary of the investigation, including the status of all blood donors if a look-back study was conducted, should be sent to the CDC point-of-contact.

APPENDIX C
TRANSPLANT INVESTIGATIONS

1) Conduct a routine NIR investigation using Modules A and B.

2) Obtain a transfusion history.

3) Verify receipt of the transplant through the facility where the transplant took place.

4) Contact the transplant coordinator at the facility.

5) Identify source of transplant. Contact the organ harvesting center.

6) Check other recipients of tissues/organs from the same donor for HIV serostatus.

APPENDIX D

INVESTIGATION OF SEXUAL TRANSMISSION IN CHILDREN

1) HIV/AIDS Surveillance Definition for **Confirmed** Sexual Exposure to HIV Infection in Children.
To meet this definition, a child must have:

- Confirmed HIV infection or AIDS, AND
- A diagnosis of sexual abuse (i.e., genital-genital, genital-anal contact) based on at least one of the following:
    - Physical examination or physician diagnosis
    - Child, caregiver, or perpetrator disclosure
    - Previous or concurrent non-congenital sexually transmitted disease (e.g., syphilis, gonorrhea, condyloma, etc)
    - Prosecution of perpetrator
    - Pregnancy, AND
- Documentation in perpetrator of:
    - HIV infection or AIDS, OR
    - Risk for HIV infection:
        - male-to-male sexual contact
        - injecting drug use
        - hemophilia/coagulation disorder
        - transfusion/transplant recipient with documented HIV infection

2) HIV/AIDS Surveillance Definition for **Suspected** Sexual Exposure to HIV Infection Among Children.
To meet this definition a child must have:

- Confirmed HIV infection or AIDS, AND
- A diagnosis of sexual abuse as noted above, AND
- No other risk factor for HIV

These cases may not meet the confirmed definition of sexual abuse because the following information was not available: the identity, HIV serostatus, or HIV risk of the perpetrator.

INFORMATION TO COLLECT IN A PEDIATRIC CASE INVESTIGATION

1) Basic Demographics
   - Age
   - Race/Ethnicity
   - Parental (biologic) race
   - Country of birth
   - Parental (biologic) country of birth
2) School/Living/Occupational History (since birth)
   - Day care attendance
   - School attendance
   - Foster care placement
   - Types, dates, and location of any job held
3) Medical history (since birth)
   - Date HIV infection confirmed
   - Dates and results of all HIV testing
   - Reason for HIV testing
     - Documented or suspected HIV infection in the parent(s)
     - Presentation with symptoms consistent with HIV
     - Recipient of blood/blood products or transplant
     - Dialysis recipient
     - Parental/caregiver request
     - Social service agency initiated
     - Positive neonatal drug screen
     - Routine screening
   - Hospitalizations (emphasis on description of neonatal course)
   - Surgeries (including surgeon's name)
   - Dental surgery or treatment (including dentist's name)
   - Receipt of blood or blood products/components
   - Receipt of any immune globulin
   - Organ transplant
   - Dialysis
   - Acupuncture
   - Medical conditions requiring injections (i.e., growth hormone, steroids)
   - Injections by non health care personnel
   - Any activities involving needles, knives, blood
   - Sexually transmitted diseases (GC, syphilis, chlamydia, herpes, venereal warts, urethritis, genital ulcers)
   - Hepatitis, hepatitis vaccine, hepatitis immune globulin
   - Hepatitis B serology on parents and child
   - Chronic skin disease (eczema, seborrhea)
   - Bites or blood contact (any setting: foster care placement, school, day care)
4) Travel history (since birth) outside the US (medical care, injections, sexual contacts)
5) Illicit drug use history (this checklist should apply to parent or child with illicit drug use history and include time period in the past 10 years and before diagnosis of child's HIV infection)
   - Ever visited a drug 'shooting gallery'
   - Ever visited a 'crack house'
   - Use of crack, cocaine, heroin, crank, speed, barbiturates, PCP, any other drug
   - Ever used any drug intravenously

- Ever used drugs by skin popping

6) Sexual history (since time period for which child acknowledges sexual contact)

- Number and name of opposite and same sex contacts
- Ever accepted drugs, money for sex
- History of sexual abuse, rape
    - Report filed with police or children's protection agency
    - Physician record with documentation of genital-genital or genital-anal sex (e.g., hymenal distortion as reported by a physician familiar with pediatric introitus anatomy, anal lacerations, vaginal lacerations, perineal bruising, etc)
    - Child's verbal affirmation of sexual assault/penetration
    - Adult caregiver's or perpetrator's verbal affirmation of sexual assault/penetration
    - Documentation of concomitant or previous non-congenital sexually transmitted disease (GC, syphilis, venereal warts, genital ulcers, herpes, chlamydia, urethritis, trichomonas)
    - Resultant pregnancy
    - Prosecution of perpetrator for genital-genital or genital-anal sexual contact
- Any sex partners/perpetrators:
    - HIV/AIDS
    - Bisexual
    - Intravenous drug user
    - Received blood or blood product/components
    - Received transplant or artificial insemination
    - Born outside US
    - Ever accepted drugs, money for sex
- Any sex partners/perpetrators had sex with any person in the above high risk groups (section VII/D)

7) Parent's history (time period after last negative HIV test or last 10 years and before child's diagnosis of HIV infection)

- Illicit drug use
- Receipt of blood or blood products
- Organ transplant
- Dialysis
- Medical conditions requiring injections (i.e., pituitary hormone, steroids)
- Artificial insemination
- Injections by non health care personnel
- Any activities involving needles, knives, blood
- Sexually transmitted diseases (GC, syphilis, chlamydia, herpes, venereal warts, urethritis, genital ulcers)
- Employed in any health care facility or clinical laboratory
- Accepted money or drugs for sex
- Sexual partners at high risk
    - HIV/AIDS
    - Bisexual
    - Intravenous drug user
    - Received blood or blood product
    - Received transplant or artificial insemination
    - Born outside the US
    - Ever accepted money or drugs for sex
- History of rape
- Travel outside of the US (medical care, injections, sexual contacts)

8) Prison/jail history of the parent (in the last 10 years and before the child's diagnosis of HIV infection)

- Specify reason for incarceration
- Drug use
- Sexual contacts including rape

9) Social history of the parent: Was there ever a referral to a children's protective agency for neglect or abuse?

- Hospital or physician referral
- School referral
- Neighbor referral
- Relative referral

10) Household contacts

- Any HIV-infected household members/caretakers; any known HIV-infected visitors to
- household (describe contact with child)
- Any home health care taking place (needles or other medical sharps in household)
- Exposure to open wounds/cracked skin of HIV-infected household members
- Any sharing of previously chewed food
- Bowel and bladder control
- Household cleansing practices (linen, medical care, physical care, shared toothbrush, shared razors)
- Shared eating utensils
- Shared sleeping facilities
- Shared cleansing utensils (oral, skin, hair, razor, etc)
- Shared clothing

APPENDIX E

INVESTIGATION OF SUSPECTED OCCUPATIONAL EXPOSURES

Reports to CDC of occupational exposures are generated through several different mechanisms:

1) Post-exposure prophylaxis (PEP) failures
2) State health department notification
3) Health care provider calls
4) Health care worker calls
5) Health care worker identified in HIV/AIDS Reporting System (HARS)

Investigations of suspected occupational exposures are handled as ‘routine No Identified Risk’ cases but should be investigated using Module C, “Assessment Form for HIV/AIDS Cases Reported with Possible Occupationally Related Exposure to HIV.”

APPENDIX F

HIV-2 CASE DEFINITION[1]

The CDC algorithm for testing recommends HIV-2 testing only in cases where:

HIV-1 Western blot results are negative or indeterminate following a positive HIV-1 & 2 EIA or with an unusual indeterminate pattern after a positive HIV-1 EIA with *gag* (p55, p24, or p17) plus *pol* (p66, p51 or p32) bands in the absence of *env* (gp160, gp120, or gp41) bands

OR

A patient tests positive on a licensed EIA test (including licensed rapid tests) that discriminates HIV-1 from HIV-2 (HIV-2 EIA)

AND

The patient has epidemiologic risk factors associated with HIV-2 infection listed below:

If a patient tests positive on HIV-1 western blot, no further testing for HIV-2 is recommended based on current CDC guidelines.

Persons at risk for HIV-2 include:

1. Sex partners of a person from a country where HIV-2 is endemic (this includes persons originally from such countries)
2. Sex partners of a person known to be infected with HIV-2
3. Persons who received a transfusion of blood or a non-sterile injection in country where HIV-2 is endemic[2]
4. Persons who shared needles with a person from a country where HIV-2 is endemic or with a person known to be infected with HIV-2
5. Children of women who have risk factors for HIV-2 infection or who are known to be infected with HIV-2.

Additionally, testing for HIV-2 is indicated when there is clinical evidence for or suspicion of HIV disease (such as an AIDS-associated opportunistic infection) in the absence of a positive test for antibodies to HIV-1 and in cases of an indeterminate HIV-1 Western blot as described above. Or, persons with documented HIV infection and clinical deterioration with persistently undetectable viral load.

[1]Testing for Antibodies to Human Immunodeficiency Virus Type 2 in the United States. MMWR July 17, 1992/ 41 (RR12); 1–9

At this time, no Western Blot tests are licensed in the U.S. for the diagnosis of HIV-2

CDC confirms a case using the following:

- Positive result on the Canadian Select HIV 1 & 2 test—the Canadian Select uses separate plates for HIV-1 and HIV-2
- If the HIV-2 plate is positive, an HIV-2 Western Blot* is done if the kit is available

- Or, confirmation with the Biorad Multispot Rapid Test if WB kit not available

*Genlab—purchased through Singapore (not available in the U.S.)

If requested a qualitative HIV-2 RNA test (unlicensed) can be performed in the CDC laboratory.

Probable case:

Both must apply:

- Statement in the medical record by a physician that the patient tested HIV-2 positive (and details of how that diagnosis was made)
- An epidemiologic picture consistent w/ HIV-2 risk factors listed above

Potential cases not covered under the criteria listed above will be handled on a case-by-case basis.

[2]Countries where HIV-2 is prevalent (+ indicates more than 1% HIV-2 prevalence in the general population):
West African nations:

Benin	Mauritania+
Burkina Faso	Niger
Cape Verde+	Nigeria+
Code d'Ivoire+	Sao Tome
Gambia+	Senegal
Ghana	Sierra Leone+
Guinea	Togo
Guinea-Bissau+	
Liberia	Other African Nations: Angola+, Mozambique+
	Mali+ Other countries where HIV-2 has been reported: Portugal, France, India, Brazil, Canada and the United States

Appendix B:
Risk Factors

Risk Factors

Risk factors for adults/adolescents:
Currently, the introduction to the patient history section of the adult case report form (CDC 50.42A) states "After 1977 and preceding the first positive HIV antibody test or AIDS diagnosis, this patient had…." *Technical Guidance for HIV/AIDS Surveillance Programs* changes the introductory statement to "Before the earliest known positive HIV test or AIDS diagnosis, this patient had…." If the person was exposed to HIV infection by any of the following routes before his/her first positive HIV test or AIDS diagnosis, then it is considered a CDC-defined risk factor for HIV infection:

1. Male who had sex with another male: This wording is intended to avoid the issue of sexual orientation or identity (whether the man considered himself homosexual, bisexual, "gay," "on the down-low," or basically heterosexual but occasionally having sex with other men). The important consideration here is not how this male perceived himself, but simply whether he had sex with another man. In this context, "having sex" or "sexual contact" means penis-to-mouth, penis-to-anus, or mouth-to-anus contact (but not mouth-to-mouth contact) regardless of which role (insertive or receptive) is played by the male in question. It does not include contact only with skin (not a body orifice). However, if explicit information on whether the man had sex with another man is unavailable, the man may be assumed to have done so if he stated that he was "homosexual" or "bisexual" or described himself with a similar term that implies that he had sex with another man. In addition, male-to-male sex may be inferred if he was diagnosed with any rectal STD (e.g., gonorrhea) before or at the time of HIV/AIDS diagnosis.

2. Injected illicit or nonprescribed drug(s): This means receiving an injection, either self-administered or given by another person, of a drug that was not prescribed by a physician for this person. It generally includes illicit drugs used for producing euphoria, but it may also include prescription drugs that were not prescribed (e.g., estrogen, testosterone, anabolic steroids, or human growth hormone). It does not include injection of prescribed drugs (e.g., insulin for treating diabetes). The drug itself is not the source of the HIV infection, but the context of it being taken illicitly (i.e., without a prescription) is likely to be associated with sharing of injection equipment (e.g., syringes, needles, cookers), which can result in transmission of bloodborne pathogens, such as HIV. The case report form does not include a separate question asking if injection equipment was shared.

3. Had sex with someone of the opposite sex who had either of the two risk factors listed previously in items 1 or 2 (MSM and/or IDU): In this context, "having sex" or "sexual contact" means contact of one person's penis or mouth with the vagina or anus or penis of another person. It does not include mouth-to-mouth contact or contact of the penis or mouth with skin (not a body opening). Because the prevalence of HIV infection is high among men who have had sex with men and among injection drug users, such sex partners will be presumed to have HIV infection and it will not be necessary to document their infection.

4. Had sex with someone of the opposite sex who was diagnosed with HIV infection or AIDS after having any risk factor for HIV infection listed below in items 6 (receipt of clotting factor for coagulation disorder), 7 (receipt of blood transfusion), or 8 (receipt of transplant or artificial insemination): Having sex is defined as previously in item 3. Because HIV infection has an extremely low prevalence among recipients of clotting factors who were born in March 1985 or after, recipients of blood transfusions, and recipients of transplants or artificial insemination, such sex partners will not automatically be presumed to have HIV infection. Instead, their HIV infection must be documented (e.g., by the history given by the person being reported as a case to his/her health care provider), but it does not require confirmation by a special investigation. For the sex partner's HIV infection to be attributed to any of these risk factors (e.g., receipt of clotting factor, transfusion, or transplant), the sex partner's diagnosis of HIV infection or AIDS should have occurred after the sex partner's exposure to these risk factors (the exposure must not have occurred only after the diagnosis). If the time relationship between the sex partner's HIV infection diagnosis and the sex partner's exposure to the risk factor cannot be ascertained, the risk factor may be assumed to have preceded the sex partner's diagnosis.

5. Had sex with someone of the opposite sex who was diagnosed with HIV infection or AIDS but was not known to have had any of the risk factors of sex partners described above in items 3 and 4: Having sex is defined as previously in item 3. The sex partner's HIV infection or AIDS must be documented (e.g., by the history given by the person being reported as a case), but it does not require confirmation by a special investigation.

6. Received clotting factor injection for hemophilia or another coagulation disorder: This mainly involves Factor VIII and Factor IX. In the United States, screening of blood donors for antibody to HIV began in March 1985, which reduced the likelihood that clotting factor obtained after that month would be contaminated with HIV. In addition, clotting factor blood products for hemophilia began to be more effectively heat-treated around that time. More recently, clotting factors have been synthesized without using donated blood. Therefore, it would be unexpected for persons with hemophilia born in or after March 1985 to acquire HIV infection by this route, and such an occurrence must be confirmed by an investigation under the protocol for cases of public health importance (COPHI).

7. Received transfusion of blood or blood components (e.g., platelets): Because screening of blood donors in the United States for antibody to HIV began in March 1985, it would be unexpected for persons who received a transfusion in or after March 1985 to acquire HIV infection by this route. Therefore, such an occurrence must be confirmed by an investigation under the protocol for cases of public health importance (COPHI).

8. Received a transplant of tissue or organ or artificial insemination: Because of its rarity and public health implications, any acquisition of HIV by this route must be confirmed by an investigation under the protocol for cases of public health importance (COPHI).

9. Worked in a health care or clinical laboratory setting with possible exposure to human blood or other body fluids: This has been reworded to clarify that it includes work that involves physical contact with patients, blood, or body fluids. For example, it does not include work as a clerk, secretary, or administrator who does not have physical contact with patients. It may include a custodian, however, who could be exposed to contaminated materials that have been discarded. Because of its rarity and public health implications, any acquisition of HIV by this route must be confirmed by an investigation under the protocol for special cases of public health importance (COPHI).

10. Other exposure to human blood or body fluids: This could include other forms of occupational exposure, such as that experienced by a police officer or fire fighter, or non-occupational exposures, such as contact with another person's blood or an open wound as a result of providing informal health care to another person or as a result of a fight. Any acquisition of HIV by this route must be confirmed by an investigation under the protocol for special cases of public health importance (COPHI).

Risk factors for children:

1. Perinatal (mother-to-child) exposure with specified maternal risk factors: The child's mother had any of the risk factors described previously in items 2–5 or 7, or 8 in adult risk factors before her first positive HIV test or AIDS diagnosis, and the mother was not known to be uninfected after the child's birth:

- Maternal injection drug use
- Maternal sexual contact with a man known to have had HIV infection or who
- was at high risk because he
    - was an injection drug user, or
    - was a man who had sex with other men, or
    - had HIV infection after having received clotting factor blood products, a transfusion, or a transplant
- Maternal receipt of a transfusion (and mother known to have had HIV infection)
- Maternal receipt of a transplant (and mother known to have had HIV infection)
- Maternal receipt of clotting factors (item 6 of adult risk factors) is not included among these possible maternal risk factors because hemophilia tends to be an X-linked hereditary disorder that does not occur among females. If the mother's experience of one of these risk factors is known to have occurred only after her diagnosis of HIV infection or AIDS, then it should not be accepted as the route by which she became infected.
- Maternal perinatal exposure

2. Perinatal (mother-to-child) exposure without specified maternal risk factors: The child's mother has or had (if deceased) HIV infection or AIDS, but she was not known to have any of the risk factors described previously in items 2–5 or 7, or 8 of adult risk factors before her first positive HIV test or AIDS diagnosis, and she was not known to have been uninfected after the child's birth.

3. Risk factors for children, other than the mother's HIV infection: These all require confirmation under the protocol for special cases of public health importance (COPHI).

- Received clotting factor injection for hemophilia or another coagulation disorder: This is defined as previously in adult risk factor item 6.
- Received transfusion of blood or blood components (e.g., platelets): This is defined as previously in adult risk factor item 7.
- Received a transplant of tissue or organ or artificial insemination: This is defined as previously in adult risk factor item 8.
- Sexual abuse by an HIV-infected adult: This is defined as sexual contact of the child with a man or woman who had HIV infection or AIDS. The case report form asks if the child had sexual contact with a male or a female, but does not ask if that sex partner had HIV infection, because it is expected that the infection status of the perpetrator of the sexual abuse may not be known when the form is initially completed. A “yes” answer to the question about sexual contact will then result in an investigation under the COPHI protocol, which should reveal the infection status of the sex partner. So far, no case of pediatric HIV infection or AIDS has been reported in which a child had sex with a female; so in practice, this risk factor is limited to sexual abuse by an HIV infected man.
- Injected illicit or nonprescribed drug(s): This is defined the same as previously in adult risk factor item 2, except that its rarity in children requires it not be accepted as such until it is confirmed by COPHI investigation.
- Other exposure to human blood or body fluids: This is similar to adult risk factor item 10. Such exposures among children may involve physical contact between children while playing or fighting, in which blood or serum from an injury of one child may come into contact with an open wound of the other child.

Appendix C:
Transmission Category

Transmission Category

"Transmission category" should be the term for summarizing the multiple risk factors (as defined in risk factors) that an individual may have had by selecting the one through which HIV was most likely to have been transmitted. The selection of the most likely route of transmission is based on a presumed hierarchical order of transmission that was developed in the early years of the AIDS epidemic, and was based on what was known at the time about how HIV was transmitted. The hierarchy has not changed even though our understanding of the most efficient ways of HIV transmission has changed. The expanded transmission category variable has 5 categories of heterosexual contact (HTC), which differ by the risk factor of the sex partner, and 8 categories of perinatal (mother-to-child) exposure, which differ by the risk factor of the mother. In the transmission category variable (not expanded), the 5 categories of HTC are combined into a single category and the 8 categories of perinatal exposure are combined into a single category. For cases in which there were multiple risk factors, the hierarchical nature of this classification may conceal some risk factors. For example, with a combination of IDU and HTC, only the IDU would be selected and the HTC would be hidden. An exception to the hierarchy is made for the combination of MSM and IDU, in which one of those two risk factors is not selected over the other and both are presented in a combination category. The transmission category and expanded transmission category variables include some categories that come in pairs—one for adults/adolescents and another for children—for 1) receipt of blood transfusion/transplant, 2) receipt of blood products for treatment of hemophilia, 3) "other" risk factors, and 4) absence of reported/identified risk factors. The list of categories in the transmission category classification is shown in Table 1:

Table 1: Distribution of US AIDS cases reported through 2003 by transmission category

Transmission Category	Frequency	Percent
MSM	373257	44.22
IDU	203226	24.08
MSM & IDU	49915	5.91
Adult Hemophiliac	4633	0.55
HTC	105616	12.51
Adult Transfusion*	8777	1.04
Adult Other	29	0.00
Adult Undetermined	88964	10.54
Pediatric Hemophiliac	563	0.07
Mother w/HIV	8353	0.99
Pediatric Transfusion*	415	0.05
Pediatric Other	20	0.00
Pediatric Undetermined	299	0.04
Total†	844067	100.00

* Receipt of a blood transfusion, donated organ or tissue, or artificial insemination.
† Excluding cases reported from more than one health department.

Chapter 4 Case Ownership

4-1 Case Ownership Assignment

HIV/AIDS cases are assigned jurisdictional case ownership based on the place of residence at current diagnostic status. If a case's diagnostic status changes (e.g. progresses from HIV to AIDS) then case ownership is reassigned based on the residence of diagnosis at the most current diagnostic status. Case ownership is determined solely on the city, county and zip code information that is entered into the **Residence at Diagnosis** section of the CRF at the time of the first HIV or AIDS defining diagnosis. Case ownership is not based on any other information, including jurisdiction of data entry, jurisdiction completing the CRF, jurisdiction of care, stateno or current residence.

Once a case is assigned a stateno, the stateno will never change regardless of updated jurisdiction. For cases that progress to AIDS in a different jurisdiction from residence at HIV diagnosis, the residence at AIDS diagnosis will be updated but the stateno will not change.

It is important to note that eHARS has several application-specific ownership calculations: primary case ownership, secondary case ownership and primary document ownership. These eHARS calculations are only used within the application and have no effect on funding or other statistical calculations performed. Jurisdictional case ownership, as described above, is not affected by the eHARS calculations and is calculated outside the system for all funding and statistical analysis purposes. To learn more about the eHARS ownership calculations refer to the *Introduction to eHARS, the HIV/AIDS Reporting System* manual.

4-2 Determining Residence at Diagnosis

To determine the **Residence at Diagnosis** of a case, use the "usual residence" of the case at the time of diagnosis. The "usual residence" of the case can be assumed to be the address given by the person at the time of diagnosis, recorded in the medical chart or other document source.

According to the Council of State and Territorial Epidemiologists, the concept of usual residence is defined as:

> *The place where the person lives and sleeps most of the time, which is not necessarily the same as the person's voting residence, legal residence, or the place where they became infected with a reportable disease.*
> *Determining usual residence for most people is easy and unambiguous.*

However, in some instances "usual residence" can be ambiguous. If "usual residence" is ambiguous, jurisdictions should discuss the situation to come to an agreement on one "usual residence" at the time of diagnosis. If jurisdictions are unable to determine the "usual residence" of a case, contact Central Office for further guidance. Below are some guidelines for assisting in the determination of "usual residence." Although these guidelines were written to determine whether or not a case is a Texas resident, these same guidelines should be used to determine whether a case belongs to particular jurisdiction within Texas as well.

A. Who is a Texas Resident?

A resident of Texas meets any of the following criteria:

- Is physically present and living voluntarily in this state
- Is not in the state for temporary purposes
- Intends to make a home in this state, which may be demonstrated by the presence of personal effects at a specific abode in the state
- Employment in the state
- Possession of a Texas driver's license
- Texas motor vehicle registration
- Other similar or pertinent evidence such as utility bills in their name for a Texas address.

B. What defines a "Usual Residence"?

1. **People away on vacation or business**

People temporarily away on vacation or a business trip at the time of disease onset should be reported by the jurisdiction of their usual residence

2. **People without housing**

People without a usual residence should be reported by the jurisdiction where they were staying on the day of diagnosis.

3. **People with multiple residences**

a. **Commuter –** workers living away part of the week while working (on a weekly cycle) should be reported by the jurisdiction where they stay most of the time.

b. **Snowbirds –** People who live in one state most of the year but who regularly spend part of the year in another state can be said to have an annual cycle and should be reported by the jurisdiction of the residence where they live most of the time.

c. **Children in joint custody –** should be reported by the jurisdiction of the residence where they live most of the time. If the time is equally divided, they are reported by the jurisdiction where they were staying at the time of disease onset.

d. **Multiple residences –** people who move between residences without any regular cycle should be reported by the jurisdiction of the residence where they live most of the time. If their time is equally divided, report based on where they were staying at the time of disease onset.

4. **Students**

a. College or boarding school students on a typical yearly academic cycle should be reported by the jurisdiction of the residence where they live most of the year.

b. If the individual is an intermittent or part-time student without regular cycle for moving between parental and school residences, then report by the jurisdiction where they were living at the time of disease onset.

5. **Live-ins**

Foster children should be reported by where they were living at the time of disease onset.

6. **Military or merchant marine personnel in the U.S.**

a. People in the military residing in the United States residency should be

assigned by using the address where they were living at the time of diagnosis, either on the base or off the base

b. Crews of military vessels with a U.S. homeport should be reported by the jurisdiction at the usual onshore residence if they report one (the place where they live and sleep most of the time when they are onshore) otherwise, at their vessel's homeport.

c. Crews of U.S. flag merchant vessels engaged in inland waterway transportation should be reported at their usual onshore residence (the place where they live and sleep most of the time when they are onshore).

d. Crews of U.S. flag merchant vessels docked in a U.S. port or sailing from one U.S. port to another U.S. port should be counted at their usual onshore residence if they report one (the place where they live and sleep most of the time when they are onshore).

7. **Institutionalized persons**

a. For persons who are incarcerated in state or federal correctional facilities at the time of diagnosis, residence of diagnosis should be defined as the residence of the correctional facility.

b. For persons who are incarcerated in city or county jails for short-term stays (a year or less), place of residency should be assigned by using the home address. Facility address should only be used if home address is not available.

c. Patients in general hospitals or wards at the time of diagnosis should be reported by the jurisdiction of their usual residence **(the place where they live and sleep most of the time when they are not hospitalized).** Newborns that have not yet been discharged following delivery should be reported by jurisdiction of the mother's usual residence.

d. In general, persons who are institutionalized for indefinite or long-term stays should be reported by the jurisdiction of the facility where they are staying at the time of disease onset. Examples of such facilities include:

Chronic or long-term disease hospitals
Hospices
Nursing or convalescent homes
Inpatient drug/alcohol recovery facilities
Homes, schools, hospitals or wards for the physically handicapped, mentally retarded, or mentally ill.
Federal and state prisons, jails, detention centers and halfway houses
Orphanages
Residential care facilities for neglected or abused children.

c. Staff members living in hospitals, nursing homes, prisons, or other institutions should be reported by the jurisdiction of their usual residence (the place where they live and sleep most of the time); otherwise by the jurisdiction where the institution is located.

8. **Foreign citizens**

Individuals who are diagnosed in the U.S. with a notifiable disease, should be reported to the CDC via the state eHARS.

a. Foreign citizens who have established a household or are part of an

established household in the U.S., including those here for work or study, should be reported by the jurisdiction of their usual residence in the U.S.
b. Foreign citizens who live on diplomatic compounds (e.g., embassies, consulates) should be reported by the jurisdiction where the facility is located.

9. **U.S. residents diagnosed abroad**
When diagnosis occurs overseas, illness among U.S. residents is only notifiable in the U.S. if the patient receives care and treatment in the U.S. and the patient does not have evidence of diagnosis outside the U.S. If the patient has evidence that he/she has been diagnosed in another country, we cannot report the individual. Healthcare providers in the U.S. treating patients diagnosed with a notifiable disease while traveling or temporarily living outside the U.S. should notify their local or state health department of the continued treatment or care of a notifiable condition, along with information regarding the location where the disease was likely acquired. The case jurisdiction should be based on location of "usual residence" at the time of treatment or care.

4-3 Assigning a Stateno

All new HIV cases are assigned a unique code (stateno) based on **jurisdiction of investigation** at time of initial diagnosis. Because eHARS is a centralized system and stateno assignment has no effect on how jurisdictional case ownership is assigned, once a case has been assigned a stateno the case will never be reassigned a new stateno. If the jurisdictional ownership or investigation of a case changes, the case will retain its original stateno. Even if case ownership changes states, the case will remain in eHARS with its original stateno.

The following guidelines should be used when assigning statenos on a CRF:

1. New case forms: A new stateno should be assigned using the surveillance site code of the jurisdiction investigating the case, the year, and a unique number sequence (e.g. D0123456). The number sequence assigned is based off a log kept by each of the jurisdictions to ensure that numbers are never repeated. Refer to the list below for each jurisdiction's code that is used to start the stateno sequence.

Jurisdiction	Code
Austin	A
Cactus	T
Dallas	D
El Paso	E
Galveston	G
Houston	H
Prison	P
Region 1	Y
Region 2/3	W

Region 4/5	L
Region 6/5	J
Region 11	R11
San Antonio	S
Tarrant	FW

2. Update to AIDS or other update forms: The stateno, which has already been assigned to the case should be used.
3. OOS case forms: When completing an ACRF for an OOS case, which has not yet been reported in Texas eHARS, a Texas stateno should be assigned using the surveillance site code of the Texas jurisdiction investigating the case plus a unique number sequence. The stateno assigned by the other state should be recorded in the ID section of the ACRF.

4-4 Maintaining Out of State (OOS) Cases

All HIV cases who reside in or have HIV care in Texas during the course of their infection are entered into eHARS, even if that case is "owned" by another state.

- If a Texas HIV case is diagnosed with AIDS in another state, this case will remain in the Texas eHARS system with an OOS report document indicating that the case has been diagnosed with AIDS in another state.
- If a Texas AIDS case was diagnosed with HIV in another state, the eHARS record for this case will have an OOS report document indicating that the case was diagnosed with HIV in another state.
- If a case was diagnosed with both HIV and AIDS in another state or is an HIV only case reported by another state, but is residing in or receiving HIV services in Texas, that case will be reported to eHARS with the Texas residence and care information. Additionally, OOS report documents will be added to that case with the HIV and AIDS diagnosing information from the other state.

All cases that have been diagnosed with HIV and/or AIDS in another state will be entered into eHARS with a Texas Stateno.

A. OOS Procedures

If there is evidence that a case was reported in another state, an Out of State (OOS) Record Search can be performed by Central Office. An Out of State record search should be requested if:

- The patient told a DIS that he/she tested positive in another state
- The patient reported to their health care provider that they had tested positive in another state
- The patient is found in the Lookup File with an OOS id (this includes ELR records that are matched to the Lookup File in Central Office)

An OOS record search should not be requested based only on an out of state social security number or identification of an out of state address in Accurint. OOS record searches can be requested by calling Central Office or completing the Out of State

Request form. Please refer to *Appendix A:* ***Procedures for OOS Request***, for detailed instructions on Out of State Requests.

4-5 Prison Cases

Prison cases are defined as those cases diagnosed and/or residing in a Texas Department of Criminal Justice (TDCJ) facility or non-TDCJ correction facility in Texas, including federal prisons, county/local jails and youth correctional facilities. Adults who are inmates at TDCJ facilities are tested for HIV upon entry and exit of a TDCJ facility. Adults who are inmates at some non-TDCJ correctional facilities are tested upon entry and exit, however, this practice varies by facility. Surveillance sites are required to complete CRFs for all prison cases. However, different protocol should be followed when reporting cases diagnosed/residing in a TDCJ facility from that used to report cases diagnosed/residing in a non-TDCJ facility. When completing a CRF for any prison case, be sure to include the address of the prison facility if the case is a long-term resident of the facility.

A. **TDCJ cases:** Surveillance staff are responsible for reporting TDCJ cases in TDCJ facilities in their region. A medical record abstraction is not required at the TDCJ facility. However, surveillance staff should complete a CRF based on any case information obtained through a DIS interview or STD*MIS notes. Surveillance staff do not need to assign a Stateno to TDCJ cases, as the Stateno will be assigned by Central Office. Surveillance staff should clearly distinguish TDCJ cases from other cases when sending CRFs to Central Office so the CRFs can be routed to the appropriate TDCJ data entry staff. To ensure that all prison cases are reported, the TDCJ Central Contact also completes and sends CRFs for cases diagnosed with HIV and/or AIDS to Central Office. TDCJ has asked that the surveillance staff remind and encourage local TDCJ unit medical personnel to report HIV/STD cases to the TDCJ Central Contact. Once any TDCJ CRF arrives at Central Office, TDCJ data entry staff record search and data enter all information into eHARS.

A listing of TDCJ prison units, addresses and counties can be found in *Appendix B: TDCJ Unit Names* and map of TDCJ facilities can be found in *Appendix C: TDCJ Facility Map* In addition, a list of the TDCJ prison units are online at: http://www.tdcj.state.tx.us/stat/unitdirectory/all.htm

B. **Non-TDCJ cases:** All prison and jail HIV/AIDS cases that are not a part of the TDCJ system (i.e. city, county, or federal correctional facilities) are reported by the jurisdiction in which the correctional facility is located. To report non-TDCJ inmates who test positive for HIV/AIDS, please refer to Chapter 1.

4-6 Out of Jurisdiction Policy

Many patients receive care in the same jurisdiction as they live. However, there are circumstances where a case may live in one jurisdiction within Texas and receive care in another jurisdiction within Texas (OOJ Cases). The jurisdiction where the case lives

receives the initial laboratory report on the case and has ultimate responsibility for collecting case information. However, it can be challenging to collect case information from providers in another jurisdiction. The following procedure should be used to obtain and transmit information between jurisdictions:

1) A lab will be sent to the jurisdiction where the case lives (unless no address is listed for the case). Once received, the site should request a medical record abstraction from the jurisdiction where the case is receiving care within 3 business days. Abstraction Requests should be completed and posted on the TXPHIN. An email should be sent to the site where the case is receiving care to notify surveillance staff of the Abstraction Request. Labs should be transmitted to the jurisdiction where the case receives care. If the jurisdiction where the case is receiving care is in the Cactus regions, a request should be sent to the Cactus coordinator.

2) When the jurisdiction where the case is receiving care receives the Abstraction Request, surveillance staff should immediately schedule a medical record abstraction. Surveillance staff should provide necessary documentation to the requesting site within 7 days for reportable lab results and within 45 days for a non-detectable Viral Load CD4 count/percent. The following documents must be completed by the jurisdiction where the case is receiving care:
   a. A Case Report Form based on the medical record abstraction
   b. A complete Medical Record Worksheet (See Appendix D)
   c. The Case Report Form should be sent to Central Office. A courtesy copy should be provided to the site where the case lives. The courtesy copy must include "COPY" at the top of the first page of the Case Report Form. This is provided for informational purposes only and should not be entered into eHARS or routed for entry.

   The Medical Record Worksheet should be provided to the site where the case resides.

3) If the site where the case receives care cannot provide information back to the requestor within the above timeframes for reasons outside of the site's control (such as problems scheduling medical record reviews at a provider's office), the site will provide the requestor with a reasonable date by which the information can be provided. Any date extensions must be provided to the requesting site via email.

4) If the requesting site has not received documentation within the above timeframe (7 days for reportable laboratory results and 45 days for a non-detectable Viral Load CD4 count/percent) and no notification of date extensions have been received, the requesting site will send a follow up email that includes the dates the information was requested and the number of records requested. Program managers from both programs should be included on the email.

5) If a follow up email has been sent and, after 7 days the requesting site has not received documentation, , a formal email should be sent to the jurisdiction where

the case is receiving care and Central Office that documents the dates that requests were made and the number of outstanding medical record reviews.

6) All Case Report Forms will be entered by the site that completes the form. Thus, it is possible that two sites will enter separate pieces of information on one case. For example, one case report form may be completed by the jurisdiction where the case is receiving care based on the medical record abstraction. A separate case report form may be completed by the jurisdiction where the case is living, based on the DIS interview. In this scenario the data entry staff for the jurisdiction where the case is receiving care will enter the information from the medical record abstraction and the data entry staff for jurisdiction where the case is living will enter information from the DIS interview.

Less Common Scenarios:

- If the original lab is sent to the jurisdiction where the case is receiving care because no residential address is listed on the lab, item 2 above should be followed to provide case information to the jurisdiction where the case lives (as identified by in the medical record). In addition, STD surveillance staff should be notified so appropriate protocol can be followed for public health follow up.

- If a lab is received locally from a hospital that process labs in house (not sent by Central Office), item 2 above should be followed to provide case information to the jurisdiction where the case lives (as identified by in the medical record).

Appendix A:
Procedures for OOS Request

Procedures for OOS Request

The following procedures should be followed when requesting an OOS record search.

1. Request an OOS record search by either calling in the request to Central Office or by sending Central Office a completed *OOS Request* form.
   a. The person requesting the OOS record search should complete the portion of the form titled *Texas Case Information,* as well as the Stateno field in the top right corner.
   b. If the OOS record search is called-in, surveillance staff should be prepared to provide Central Office with the same information. If you are calling in an OOS record search, do not contact multiple staff at central office for the same request.
   c. Surveillance sites must provide as much information as possible when requesting an OOS record search. If you complete the *Texas Case Information* section with information from a medical record abstraction or a DIS interview and the case was reported in another state, this information will be entered into eHARS with the OOS information, so it is important to be as accurate and thorough as possible when completing the form. In addition, many states expect that Central Office will provide them with the information that prompted the call (e.g. the lab report information from the Texas Facility of care). Note that if you only have the alias name for a case, you can use this name when completing the form. At a minimum, you should provide a name, date of birth, and the state in which the case was suspected to be diagnosed.
2. Once the necessary portion of the OOS Record Search Request form has been completed, surveillance sites should scan the form and place this file on the TxPHIN. A new form must be completed for each case and forms must be scanned and posted in the TxPHIN when more than 4 requests are submitted within one day. If a surveillance site does not have a scanner, Central Office can provide the site with electronic forms or surveillance sites can call Central Office to give the appropriate information.
3. Once the form is received by Central Office, Central Office staff will process the record search request, contact the other state, and respond with follow-up information on the case in 3-5 days.
   a. If the case has been reported in another state and is **not** a Texas AIDS case, Central Office will complete the lower portion of the *OOS Record Search Request* and return the information back to the requesting site. This is for informational purposes only. The site is not required to complete any additional action on the case at the time of report.
   b. If the case is a Texas AIDS case, a medical record abstraction and subsequent completion of a case report form is required. Do not include ANY information from the OOS record search results on the ACRF.
   c. If the case has not been reported in another state, central office staff will notify the site. Complete an ACRF following the same procedures as you would use for any new case. Do not use the Out of State residence as the residence at diagnosis.
4. For all OOS cases, the following documents will be entered into eHARS:
   a. An ACRF with the results of the OOS record search;

b. An ACRF with the results of a medical record abstraction, if applicable (based on what was provided at the time of request);
c. An ACRF with the results of a DIS interview, if applicable (based on what was provided at the time of request);
d. Any lab documents associated with the case.

If an OOS record search was requested because a patient was in the Out of State database or an ELR listed an OOS Stateno and the case was reported in another state, central office will only enter the OOS record search document and any lab documents associated with the case. A medical record abstraction or DIS interview is not required in this scenario, unless he/she is a Texas AIDS case.

Appendix B:
TDCJ Unit Names

Prison Unit Directory

UNIT NAME	TDCJ UNIT TYPE	ADDRESS-STREET, CITY, ZIP, COUNTY	UNIT CODE	STD SITE	TDH REG	SEX	TDCJ REG
ALLRED	TDCJ-Prison	2101 FM 369 N, Iowa Park, 76367, Wichita	JA	WF	2	M	V
BARTLETT	Private State Jail	1018 Arnold Dr Bartlett, 76511, Bell	BL	R7	7	M	II
BETO	TDCJ-Prison	P. O. Box 128, Tennessee Colony, 75880, Anderson	B	R4	4	M	II
BOWIE	Leased Bed - Contract Transfer	105 W. Front St., Texarkana, 75501, Bowie	XC	R4	4	M	II
BOYD	TDCJ-Prison	Rt. 2, Box 500, Teague, 75860, Freestone	BY	R7	7	M	II
BRADSHAW	Private State Jail	3900 W. Loop 571 N,, Henderson, 75653, Rusk	BH	R4	4	M	II
BRIDGEPORT	Private TDCJ-Prison	4000 N. 10th St, Bridgeport, 76426, Wise	BR	R3	3	M	V
BRIDGEPORT	Pre Parole	222 Lake Road, Bridgeport, 76426, Wise	TC	R3	3	F	V
BRISCOE	TDCJ-Prison	1459 W. HWY 85, Dilley, 78017, Frio	DB	R8	8	M	IV
BYRD	TDCJ-Prison	FM 247, Huntsville, 77340, Walker	DU	R6	6	M	I
CENTRAL	TDCJ-Prison	One Circle Dr, Sugarland, 77478, Fort Bend	C	R6	6	M	III
CHOICE MOORE	Transfer Facility	1700 N. FM 87, Bonham, TX 75418, Fannin	CM	R4	3	M	II
CLEMENS	TDCJ-Prison	11034 HWY 36, Brazoria, 77422, Brazoria	CN	GA	6	M	III
CLEMENTS	TDCJ-Prison	9601 Spur 591, Amarillo, 79107, Potter	BC	AM	1	M	V
CLEVELAND	Private TDCJ-Prison	P. O. Box 1678, Cleveland, 77328, Liberty	CV	R6	6	M	I
COFFIELD	TDCJ-Prison	Rt 1 Box 150, Tennessee Colony, 75884, Anderson	CO	R4	4	M	II
COLE	State Jail	Rt 3, Box 888, Bonham, 75418, Fannin	CL	R3	3	M	II
COMANCHE CO.	Leased Bed - Contract Transfer	300 Industrial Blvd. Comamche, 76442 Comanche	XI	AB	2	M	V
CONNALLY	TDCJ-Prison	HC67 Box 115, Kenedy, 78119, Karnes	CY	R8	8	M	IV
COTULLA	Transfer Facility	Rt 1, Box 100, Cotulla, 78014, La Salle	N4	R8	8	M	IV
DALHART	TDCJ-Prison	HCR4, Box 4000, Dalhart, 79022, Dallam	DH	R1	1	M	V
DANIEL	TDCJ-Prison	938 S. FM 1673, Snyder, 79549, Scurry	DL	AB	2	M	V

UNIT NAME	TDCJ UNIT TYPE	ADDRESS-STREET, CITY, ZIP, COUNTY	UNIT CODE	STD SITE	TDH REG	SEX	TDCJ REG
DARRINGTON	TDCJ-Prison	59 Darrington Rd, Rosharon, 77583, Brazoria	DA	GA	6	M	III
DAWSON	Private State Jail	106 Commerce St, Dallas, 75207, Dallas	JD	DA	3	M&F	II
DIBOLL	Private TDCJ-Prison	1604 South 1st, Diboll, 75941, Angelina	DO	R4	5	M	I
DICKENS	Leased Bed - Contract Transfer	Rt 1, Box 222, Airport Rd., Spur, 79370, Dickens	XB	R1	1	M	V
DOMINGUEZ	State Jail	6535 Cagnon Rd., San Antonio, 78252, Bexar	BX	SA	8	M	IV
DUNCAN	Transfer Facility	1502 South 1st, Diboll, 75941, Angelina	N6	R4	5	M	I
EAST TEXAS	Intermediate Sanction Facility	101 B.W. Whaley, Longview, 75601, Gregg	XQ	R4	4	M	II
EASTHAM	TDCJ-Prison	Farm Road 230, Lovelady, 75851, Houston	EA	R4	5	M	I
ELLIS	TDCJ-Prison	Rt 6, Huntsville, 77343, Walker	E	R6	6	M	I
ESTELLE	TDCJ-Prison	264 FM 3478, Huntsville, 77320, Walker	E2	R6	6	M	I
ESTES/VENUS	Private TDCJ-Prison	1100 Highway 1807 Venus, 76084, Johnson	VS	R3	3	M	V
FERGUSON	TDCJ-Prison	12120 Savage Dr, Midway, 75852, Madison	FE	R7	7	M	I
FORMBY	State Jail	970 County Rd., Plainview, 79072, Hale	FB	R1	1	M	V
FT STOCKTON	Transfer Facility	1500 IH-10 East Ft Stockton, 79735, Pecos	N5	R9	9	M	IV
GALVESTON HOSPITIAL	Medical	P. O. Box 48 Substation 1, Galveston, 77555, Galveston	HG	GA	6	M&F	III
GARZA EAST	Transfer Facility	HC02 Box 995, Beeville, 78102, Bee	NI	R11	11	M	IV
GARZA WEST	Transfer Facility	HC02 Box 995, Beeville, 78102, Bee	NH	R11	11	M	IV
GATESVILLE	TDCJ-Prison	1401 State School Rd, Gatesville, 76528, Coryell	GV	R7	7	F	II
GIST	State Jail	3295 FM 3514, Beaumont, 77705, Jefferson	BJ	BM	6	M	III
GLOSSBRENNER	SAFPF	623 S. FM 1329 , San Diego, 78384, Duval	SO	R11	11	M	IV
GOODMAN	Transfer Facility	Rt 1, Box 273, Jasper, 75951, Jasper	GG	R4	5	M	I

UNIT NAME	TDCJ UNIT TYPE	ADDRESS-STREET, CITY, ZIP, COUNTY	UNIT CODE	STD SITE	TDH REG	SEX	TDCJ REG
GOREE	TDCJ-Prison	Hwy 75 South, Huntsville, 77340, Walker	GR	R6	6	M	I
GREGG	Leased Bed - Contract Transfer	P. O. Box 4529, Longview, 75606, Gregg	XE	R4	4	M	II
GURNEY	Transfer Facility	P. O. Box 6400, Tennessee Colony, 75861, Anderson	ND	R4	4	M	II
HALBERT	SAFPF	800 Ellen Halbert Dr, Burnet, 78611, Burnet	BB	R7	7	F	IV
HAMILTON	TDCJ-Prison	200 Lee Morrison Ln., Bryan, 77807, Brazos	JH	R7	7	M	VI
HAVINS	SAFPF	500 FM 45 East, Brownwood, 76801, Brown	TH	AB	2	M	V
HENLEY	SAFPF	Rt 3, Box 7000, Off FM 321, Dayton, 77535, Liberty	LT	R6	6	F	III
HIGHTOWER	TDCJ-Prison	Rt 3, Box 9800, Dayton, 77535, Liberty	HI	R6	6	M	III
HILLTOP	TDCJ-Prison	1500 State School Rd Gatesville, 76598, Coryell	HT	R7	7	F	II
HOBBY	TDCJ-Prison	742 FM 712, Marlin, 76661, Falls	HB	R7	7	F	II
HODGE	MROP	P. O. Box 999, Rusk, 75785, Cherokee	HD	R4	4	M	II
HOLLIDAY	Transfer Facility	295 IH 45N, Huntsville, 77340, Walker	NF	R6	6	M	I
HUGHES	TDCJ-Prison	Rt 2, Box 4400 (FM 929), Gatesville, 76597, Coryell	AH	R7	7	M	II
HUNTSVILLE	TDCJ-Prison	815 12th St, Huntsville, 77340, Walker	HV	R6	6	M	I
HUTCHINS	State Jail	1500 E. Langdon Rd., Dallas, 75241, Dallas	HJ	DA	3	M	II
HUTTO	Leased Bed - Contract Transfer	1001 Welch , Taylor, 76574, Williamson	XA	R7	7	M	II
JEFFERSON	Leased Bed - Contract Transfer	1001 Pearl St., Beaumont, 77704, Jefferson	XF	BM	6	M	III
JESTER I	SAFPF	Rt 2, Richmond, 77469, Fort Bend	J1	R6	6	M	III
JESTER III	TDCJ-Prison	Rt 2, Richmond, 77469, Fort Bend	J3	R6	6	M	III
JESTER IV	Psychiatric	Rt 2, Richmond, 77469, Fort Bend	J4	R6	6	M	III
JOHNSTON	SAFPF	703 Airport Rd, Winnsboro, 75494, Wood	JT	R4	4	M	II
JORDAN	TDCJ-Prison	1992 Hilton Rd, Pampa, 79065, Gray	JN	R1	1	M	V
KARNES	Leased Bed - Contract Transfer	810 Commerce St., Karnes City, 78118, Karnes	XG	R8	8	M	IV

UNIT NAME	TDCJ UNIT TYPE	ADDRESS-STREET, CITY, ZIP, COUNTY	UNIT CODE	STD SITE	TDH REG	SEX	TDCJ REG
KEGANS	State Jail	707 Top St., Houston, 77002, Harris	HM	HO	6	M	III
KYLE	Private TDCJ-Prison	701 South I35, Kyle, 78640, Hays	KY	R7	7	M	IV
LANE MURRAY	TDCJ-Prison	1916 N HWY 36 Bypass, Gatesville, 76596, Coryell	LM	R7	7	F	II
LE BLANC	TDCJ-Prison	3695 FM 3514, Beaumont, 77705, Jefferson	BA	BM	6	M	III
LEWIS	TDCJ-Prison	P. O. Box 9000 Woodville, 75990, Tyler	GL	R4	5	M	I
LIMESTONE CO.	Leased Bed - Contract Transfer	910 Tyus, Groesbeck, 76642, Limestone	XD	R7	7	M	II
LINDSEY	Private State Jail	1137 Old Post Oak Rd, Jacksboro, 76458, Jack	LN	WF	2	M	V
LOCKHART	Private TDCJ-Prison	P. O. Box 1170, Lockhart, 78644, Caldwell	LC	R7	7	F	IV
LOCKHART	Pre Parole	P. O. Box 1170, Lockhart, 78644, Caldwell	TC	R7	7	M	IV
LOPEZ	State Jail	1203 El Cibolo Rd, Edinburg, 78539, Hidalgo	RL	R11	11	M	IV
LUTHER	TDCJ-Prison	1800 Luther Dr , Navasota, 77869, Grimes	P2	R7	7	M	I
LYCHNER	State Jail	2350 Atascocita Rd., Humble, 77396, Harris	AJ	HO	6	M	I
LYNAUGH	TDCJ-Prison	Rt 1 Box 150, Ft Stockton, 79735, Pecos	LH	R9	9	M	IV
MCCONNELL	TDCJ-Prison	3001 S. Emily Dr., Beeville, 78102, Bee	ML	R11	11	M	IV
MICHAEL	TDCJ-Prison	P. O. Box 4500, Tennessee Colony, 75886, Anderson	MI	R4	4	M	II
MIDDLETON	Transfer Facility	13055 FM 3522, Abilene, 79601, Taylor	NE	AB	2	M	V
MINERAL WELLS	Pre Parole	759 Heintzelman Rd., Mineral Wells, 76067, Parker	TC	R3	3	M	V
MONTFORD	Psychiatric	8602 Peach, Lubbock, 79404, Lubbock	JM	R1	1	M	V
MOORE, B.	Private TDCJ-Prison	8500 FM N 3053, Overton, 75684, Rusk	BM	R4	4	M	II
MOORE, C.	Transfer Facility	1700 N FM 87, Bonham, 75418, Fannin	CM	R3	3	M	II
MT VIEW	TDCJ-Prison	2305 Ransom Rd, Gatesville, 76528, Coryell	MV	R7	7	F	II
MURRAY	TDCJ-Prison	1916 N Hwy 36 Bypass Gatesville, 76596, Coryell	LM	R7	7	F	II
NEAL	TDCJ-Prison	9055 Spur 591, Amarillo, 79107, Potter	KN	AM	1	M	V

UNIT NAME	TDCJ UNIT TYPE	ADDRESS-STREET, CITY, ZIP, COUNTY	UNIT CODE	STD SITE	TDH REG	SEX	TDCJ REG
NEWTON CO.	Leased Bed - Contract Transfer	Rt. 1 Box 222, Spur, 75966, Newton	XH	R4	5	M	I
NEY	SAFPF	114 Private Rd 4303, Hondo, 78861, Medina	HF	R8	8	M	IV
NORTH TEXAS	Intermediate Sanction Facility	4700 Blue Mound Road, Fort Worth, 76106, Tarrant	XL	R3	3	M	Private
PACK	TDCJ-Prison	2400 Wallace Pack Rd Navasota, 77869, Grimes	P1	R7	7	M	I
PAMPA/BATEN	Intermediate Sanction Facility	1995 Hilton Rd, Pampa, 79065, Gray	JN	R1	1	M	V
PAMPA/BATEN	TDCJ-Prison	1992 Hilton Rd, Pampa, 79065, Gray	JN	R1	1	M	V
PLANE	State Jail	Rt 3, Box 8000B, FM 686 Dayton, 77535, Liberty	LJ	R6	6	F	I
POLUNSKY	TDCJ-Prison	12002 FM 350 South, Livingston, 77351, Polk	TL	R4	5	M	I
POWLEDGE	TDCJ-Prison	Rt 2, Box 2250., Palestine, 75882, Anderson	B2	R4	4	M	II
RAMSEY I	TDCJ-Prison	1100 FM 655, Rosharon, 77583, Brazoria	R1	GA	6	M	III
RAMSEY II	TDCJ-Prison	1200 FM 655, Rosharon, 77583, Brazoria	R2	GA	6	M	III
RD RUDD	Transfer Facility	2004 Lamesa Hwy., Brownfield, 79316, Terry	RD	R1	1	M	V
RETRIEVE	TDCJ-Prison	Rt 5, Box 1500, Co Rd 290, Angleton, 77515, Brazoria	RV	GA	6	M	III
ROACH	TDCJ-Prison	Rt 2, Box 500, Childress, 79201, Childress	RH	R1	1	M	V
ROBERTSON	TDCJ-Prison	12071 FM 3522, Abilene, 79601, Taylor	RB	AB	2	M	V
SANCHEZ	State Jail	3901 State Jail Road, El Paso, 79938, El Paso	RZ	EP	10	M	IV
SAYLE	SAFPF	4176 FM 1800, Breckenridge,76424, Stephens	SY	AB	2	M	V
SCOTT	TDCJ-Prison	6999 Retrieve County Line Rd 290, Angleton, 77515, Brazoria	RV	GA	6	M	III
SEGOVIA	TDCJ-Prison	1201 E. Cibolo Rd., Edinburg, 78539, Hidalgo	EN	R11	11	M	IV
SJ DOMINGUEZ	State Jail	6535 Cagnon Rd., San Antonio, 78252, Bexar	BX	SA	8	M	IV
SKYVIEW	Psychiatric	P. O. Box 999, Rusk, 75785, Cherokee	SV	R4	4	M&F	II
SMITH	TDCJ-Prison	1313 County Rd. 19, Lamesa, 79331, Dawson	SM	R9	9	M	V
SOUTH TEXAS	Intermediate Sanction Facility	1511 Preston Road, Houston, 77002, Harris	XM	HO	6	M	Private

UNIT NAME	TDCJ UNIT TYPE	ADDRESS-STREET, CITY, ZIP, COUNTY	UNIT CODE	STD SITE	TDH REG	SEX	TDCJ REG
STEVENSON	TDCJ-Prison	1525 FM 766 , Cuero, 77954, Dewitt	SB	R8	8	M	IV
STILES	TDCJ-Prison	3060 FM 3514, Beaumont, 77705, Jefferson	ST	BM	6	M	III
STRINGFELLOW	TDCJ-Prison	1200 FM 655, Rosharon, 77583, Brazoria	R2	GA	6		III
TELFORD	TDCJ-Prison	P. O. Box 9200, New Boston, 75570, Bowie	TO	R4	4	M	II
TERRELL C.T.	TDCJ-Prison	1300 FM 655, Rosharon, 77583, Brazoria	R3	GA	6	M	III
TEXAS CITY	Medical	Rt 4, P. O. Box 1174, Dickenson,77539, Galveston	GC	GA	6	F	III
TITUS CO.	Leased Bed - Contract Transfer	304 S. Van Buren, Mt. Pleasant, 75455, Titus	XJ	R4	4	M	II
TORRES	TDCJ-Prison	125 Private Rd. 4303, Hondo, 78861, Medina	TE	R8	8	M	IV
TRAVIS CO	Private State Jail	8101 FM 969, Austin, 78724, Travis	TI	AT	7	M&F	IV
TULIA	Transfer Facility	HCR 3, Box 5C, Tulia, 79088, Swisher	N3	R1	1	M	V
VANCE	TDCJ-Prison	Rt 2, Richmond, 77469, Fort Bend	J2	R6	6	M	III
WALLACE	TDCJ-Prison	1675 S. CR 202, Colorado City, 79512, Mitchell	WL	AB	2	M	V
WARE	Transfer Facility	1681 CR 202, Colorado City, 79512, Mitchell	DW	AB	2	M	V
WEST TEXAS	Intermediate Sanction Facility	2002 Lamesa Highway, Brownfield, 79316, Terry	XN	R1	1	M	V
WHEELER	SAFPF	4300 E. 5th St., Plainview, 79072, Hale	WR	R1	1	M	V
WILLACY CO	Private State Jail	1695 South Buffalo Dr, Raymondville, 78580, Willacy	WI	R11	11	M	IV
WOODMAN	State Jail	1210 Coryell City Rd., Gatesville, 76528, Coryell	WM	R7	7	F	N/A
WYNNE	TDCJ-Prison	FM 2821, Huntsville, 77340, Walker	WY	R6	6	M	I

Appendix C:
TDCJ Facility Map

Map of TDCJ Facilities

Appendix D

Medical Record Abstraction Request

Requestor:			**Date:**	
Patient Name:				
Address:				
DOB:		**SSN:**		
Provider Name				
Address:				
Lab/s Received:				

Medical Record Worksheet

Demographics:							
Name:							
Address:							
Phone:				**Cell:**			
DOB:			**SSN:**				
Marital Status	S	M	D	W	SEP		
Provider Data							
Provider:							
Medical Record #:				**Contact:**			
Life Status:	Alive	Deceased		DOD:		State:	
Date of Test:							
Previously Tested:	Y	N	When:		Where:		
Pregnant:	Y	N		**EDC**			
Delivery Facility:							
Risk:	MSM	IDU	Sex/Female	Sex/HIV (+)	Sex/Male	Unknown	
Referred:	Y	N	Where:				
Emergency Contact:							
Phone:							
Employer:							
Phone:							
Additonal Diagnostic Data							
Viral Load:				CD4:			
Opportunistic Disease:	1).			2).			
	3).			4).			
Ancillary Record Searches							
Accurint Search:							
OOS Record Search:	Y	N	Where:				
Results:	State:		Status:	900	950		
Public Health Issues							
Sent for PHFU:	**Y**	**N**	**Date**		**FR#**		
EHARS #:							
Comments:							
Local Use							

OOJ Tracking LOG 2011

PATIENT NAME	State #	AGENCY SENT TO	DATE SENT	RESPONSE DATE	SPOKE WITH	COMPLETION DATE	COMMENTS

Updated 10/2011

Chapter 5 Test Types

Chapter 5

Chapter 5 Test Types

5-1 Laboratory Testing for HIV/AIDS

The HIV surveillance case definition is based primarily on laboratory-confirmed evidence of HIV infection, including stage 3 HIV infection (AIDS). According to the CDC's 2008 Revised Surveillance Case Definition for HIV infection, adults, adolescents and children (> 18 months) must meet one of the following laboratory standards to be reportable as an HIV positive case:
(Note: Refer to *Appendix A: Revised Surveillance Case Definitions for HIV Infection Among Adults, Adolescents, and Children Aged <18 Months and for HIV Infection and AIDS Among*
Children Aged 18 Months to <13 Years — United States, 2008, for the complete 2008 revised HIV case definition, including the diagnostic criteria for children < 18 months of age, which differs from the criteria described below).

- Positive result from an HIV antibody screening test (e.g., EIA) confirmed by a positive result from a supplemental HIV antibody test (e.g., Western blot or indirect immunofluorescence assay test).

  or

- Positive result or report of a detectable quantity (i.e., within the established limits of the laboratory test) from any of the following HIV virologic (i.e., non-antibody) tests:
  -- HIV nucleic acid (DNA or RNA) detection test (e.g., polymerase chain reaction [PCR])
  -- HIV p24 antigen test, including neutralization assay
  -- HIV isolation (viral culture)

  or

- For cases that do not meet laboratory criteria: HIV infection diagnosed by a physician or qualified medical-care provider based on the laboratory criteria and documented in a medical record. Oral reports of prior laboratory test results are not acceptable. For example, if HIV/AIDS defining labs are not present in the patient's medical record, but the physician is prescribing anti-retroviral treatment and there is a date of diagnosis listed in the patient's medical record, this would qualify as an acceptable physician diagnosis. However, if the patient stated that he/she was diagnosed in 1997, this would not be an acceptable physician diagnosis.

Currently, the standard testing algorithm for HIV includes a screening test (Section 5-2) followed by a confirmatory test for positive screening results (Section 5-3). Laboratories will conduct confirmatory tests on specimens that repeatedly yield positive results on the screening test. Other detection tests (Section 5-4) that do not require a screening and confirmatory test are also available for confirming an HIV infection.

Additionally, laboratory data (CD4+ T-lymphocyte counts or percentages) are used to classify a confirmed adult or adolescent case into one of the four HIV infection stages (stage 1, stage 2, stage 3, or stage unknown). Note that although cases with no information on CD4+ T-lymphocyte counts or percentages and no information on AIDS-defining conditions can be classified as stage unknown, staff must make every effort to

report CD4+ T-lymphocyte counts or percentages and the presence of AIDS-defining conditions at the time of HIV diagnosis.

The following laboratory standards define the HIV infection stages:

HIV Infection, Stage 1

- No AIDS-defining condition and either CD4+ T-lymphocyte count of ≥500 cells/μL or CD4+ T-lymphocyte percentage of total lymphocytes of ≥29.

HIV Infection, Stage 2

- No AIDS-defining condition and either CD4+ T-lymphocyte count of 200--499 cells/μL or CD4+ T-lymphocyte percentage of total lymphocytes of 14--28.

HIV Infection, Stage 3 (AIDS)

- CD4+ T-lymphocyte count of <200 cells/μL or CD4+ T-lymphocyte percentage of total lymphocytes of <14 or documentation of an AIDS-defining condition. Documentation of an AIDS-defining condition supersedes a CD4+ T-lymphocyte count of ≥200 cells/μL and a CD4+ T-lymphocyte percentage of total lymphocytes of ≥14.

HIV Infection, Stage Unknown

- No information available on CD4+ T-lymphocyte count or percentage and no information available on AIDS-defining conditions. (Every effort should be made to report CD4+ T-lymphocyte counts or percentages and the presence of AIDS-defining conditions at the time of diagnosis.)

Children aged 18 months to <13 years are not categorized into one of the four stages. For surveillance purposes, children aged 18 months to <13 years are classified as AIDS if the criteria for HIV infection are met and at least one of the AIDS-defining conditions has been documented.

5-2 Screening Tests

A. The ELISA (enzyme linked immunosorbent assay) Test

The ELISA (also called EIA) is the most common HIV screening test used to detect the presence of HIV antibodies. ELISA tests are most commonly used on blood samples, but can also be performed using urine, oral fluid samples, or dried blood spots. If the ELISA screening test is negative, no additional testing is done. If the ELISA screening test is positive, that result must be confirmed with a more specific test, usually a Western Blot. Note: ELISA tests are also available for other diseases such as hepatitis, so when abstracting medical charts or reviewing lab slips, ensure it is an EIA-HIV not an EIA-HBV (hepatitis B) or EIA-HCV (hepatitis C).

B. Rapid Tests

Rapid tests use a technology similar to the ELISA, but are able to produce test results in approximately 20 minutes. Currently, there are two types of rapid tests, one is used on blood specimens and the other is used on oral fluid specimens. Rapid tests have been shown to be highly accurate (99.5%) and comparable to the blood tests that are performed in a lab. All reactive rapid HIV tests must be confirmed with a Western blot or immunofluorescent assay (IFA).

5-3 Confirmatory Tests

Screening tests do not necessarily indicate HIV infection; thus, confirmatory tests must be performed to verify reactive screening test results.

A. Western Blot (WB)

Laboratories commonly use the Western blot to confirm reactive results from an ELISA or rapid HIV test. The Western blot detects the presence of HIV antibodies in specimens, which is indicated by the presence of specific bands on the Western blot strip. The primary bands that indicate an HIV infection are p24, gp41, and gp120/gp160. A positive HIV-1 Western blot must have at least two of the primary bands, while a negative HIV-1 Western blot has no bands present.

B. Indirect Fluorescent Antibody (IFA)

The IFA is also used to confirm reactive results from an ELISA or rapid test, though it is not as commonly used as the Western blot. IFA tests provide evidence of HIV infection through the binding of HIV antibodies in a specimen to HIV test antigens, which yields a fluorescent reaction.

C. Results of a Confirmatory Test

A positive result on a confirmatory HIV antibody test indicates that HIV antibodies are present and the individual is infected with HIV. A negative result on an HIV antibody test suggests that the individual is not likely infected with HIV. However, HIV antibodies may not be detectable by standard antibody tests during the first 3 to 6 weeks of infection. In some individuals, HIV antibodies may not be detectable during the first three months of infection, and in rare instances, detectable HIV antibody levels may take as long as 6 months to develop. Thus, recently infected individuals who test during the initial weeks of infection, commonly known as the “window period,” may have negative test results. Indeterminate or inconclusive test results do not indicate positive or negative results. If the Western blot or IFA confirmatory test is indeterminate, the following guidelines should be followed for re-testing:

- For blood specimens, testing should be repeated in one month.
- For oral fluid specimens, the Western blot or IFA test should be repeated using a blood specimen.

If the test results continue to be indeterminate, other tests are available to detect or rule out an HIV infection.

5-4 Other Detection Tests

Although positive HIV antibody screening tests followed by a confirmatory test is the most common procedure for identifying HIV infection, other tests can also reliably detect HIV infection, as well as monitor HIV therapy and assist in predicting disease outcome. These additional tests are also acceptable tests for reporting cases to eHARS.

A. HIV Culture

HIV culture involves the direct isolation of HIV virus from clinical specimens. Although this assay is very specific, it is rarely used because it is expensive, labor intensive and less sensitive than antibody testing. Note that the positive HIV culture is sufficient (i.e., no other test is necessary) for reporting a person as an HIV case to eHARS.

B. P24 Antigen Test

The p24 antigen test was initially developed to screen donated blood for HIV. The test detects the presence of the HIV core protein p24, which is generally only detectable in blood during the first few weeks of HIV infection (from about one week to up to three or four weeks after infection). Once antibodies begin to appear, they bind to the p24 protein, making p24 undetectable. Thus, the p24 antigen usually only yields positive results during the first 3-4 weeks of HIV infection. After this point, the p24 test may produce negative results, even for persons infected with HIV. Because the timeframe for detecting HIV with the p24 test is so limited, it is no longer the recommended test for routine screening of donated blood in the United States. The more recently developed nucleic acid test (NAT) is more sensitive and now used more commonly for screening donor blood.

The p24 antigen test employs a modified EIA technology to detect antigen, not antibody. Specimens that test repeatedly reactive to the EIA are then confirmed with a neutralization assay. Specimens that test positive on the neutralization assay are classified as positive and are considered to be from HIV-infected individuals. Note that the positive p24 test, including the neutralization assay, is sufficient (i.e., no other test is necessary) for reporting a person as an HIV case to eHARS.

C. HIV DNA and RNA PCR Tests (qualitative)

The Polymerase Chain Reaction (PCR) test detects the presence of HIV genetic material (DNA or RNA). Two types of HIV PCR tests are available: DNA PCR and RNA PCR. The entire process of extracting and testing genetic material with the PCR test is referred to as Nucleic Acid-amplification Testing (NAT). Since PCR tests look for actual virus, not antibodies, they are able to detect HIV infection much sooner than antibody tests. The PCR test can detect HIV in blood specimens within two to three weeks of infection. The RNA PCR is capable of detecting HIV several days sooner than the DNA PCR test and is frequently used to screen donor blood. DNA/RNA PCR tests are reported as “positive” or “negative” for HIV infection and no numeric value will accompany results. PCR tests may also be used to quantify the amount of genetic material in the blood (e.g. viral load test).

The PCR test is the preferred test for excluding HIV infection in children aged less than 18 months. PCR tests are not often used to screen adults for HIV because they are very expensive and difficult to administer. However, a positive (reactive) DNA or RNA PCR test is sufficient (i.e. no other test is necessary) for reporting a person as an HIV case to eHARS. Note that there are HIV PCR tests for both HIV-1 and HIV-2, but HIV-2 detection tests should be conducted through the CDC laboratory.

D. Viral Load Tests (quantitative HIV RNA PCR tests)

The viral load test measures the amount of HIV RNA in the blood of infected persons using the PCR method. Viral load testing is usually done to monitor the health of HIV-infected persons and to make antiretroviral treatment decisions.

Viral load test results are generally reported as the number of HIV copies per milliliter (ml) of blood. These results can range from "undetectable" to over a million copies per milliliter of blood. Lower numbers mean fewer viruses in the blood, while higher numbers mean more viruses in the blood. **Note: an "undetectable" viral load does not necessarily mean that the person is not HIV-infected.** Since viral load tests can only detect down to a certain level (e.g., 40 viral particles per milliliter of blood), "undetectable" may mean that the specimen contains no HIV virus or that there is not enough virus per milliliter of blood to be measured by the test (i.e., less than 40 viral copies per milliliter). In 2000, detectable viral loads were approved for reporting an HIV case in lieu of an EIA/Western blot test.

5-5 CD4 Tests

CD4+ T-lymphocyte tests measure the immunologic status of HIV-infected patients. Note that persons with other immunocompromising diseases also get CD4 tests, so CD4 test results do NOT necessarily indicate HIV infection. CD4+ cells also called T-lymphocytes, T-cells, or T-helper cells, are white blood cells that are important in fighting infections. HIV infects CD4+ cells; therefore, the number of CD4+ cells is a useful indicator of the likelihood of acquiring other opportunistic infections. The trend of CD4+ counts over time is a more important gauge of the effect of HIV on the immune system than any single CD4+ count because the counts can change from day to day. CD4+ cell counts generally decrease as HIV progresses among individuals who are not receiving treatment. A low CD4+ cell count usually indicates a weakened immune system and a higher chance of acquiring opportunistic infections. CD4+ test results are reported as CD4+ cell counts, percentages or both.

HIV positive persons with CD4+ cell counts <200 cells/µl or CD+ cell percentages <14% are classified as HIV Infection, Stage 3 (AIDS). Note that a person does not meet the HIV case definition with a CD4+ cell counts <200 cells/µl or CD+ cell percentages <14% alone, there must be laboratory-confirmed evidence of HIV infection. The CD4+ count taken at the time of diagnosis is used to classify the severity stage of a case at the time of diagnosis (see section 6-1). Highly active antiretroviral therapy may raise the CD4+ cell counts or percentages, but once an AIDS case is classified into a surveillance severity stage, they cannot be reclassified into a less severe stage.

5-6 Tests Used for Pregnancy and Newborns

A. Tests on Newborns

Since babies born to HIV positive mothers retain their mother’s antibodies for several months after birth, HIV antibody tests do not accurately diagnose HIV infection. For surveillance purposes, negative HIV antibody tests can be reported for children at or after 6 months of age in order to designate a child’s HIV infection status.The qualitative DNA PCR and RNA PCR tests may be used soon after birth to test babies born to HIV positive mothers.

B. Pregnancy and HIV Testing

Pregnancy can cause false-positive ELISA tests and indeterminate Western blot results due to cross-reacting antibodies. The most important factor in evaluating an indeterminate Western blot test result is risk assessment. Guidelines recommend a follow-up test in three months or a DNA PCR test to determine HIV infection status during and immediately following pregnancy. Surveillance staff should document negative HIV tests during pregnancy and delivery for women who first test positive during pregnancy, at delivery, or soon after delivery. Patients with indeterminate test results who are in the process of seroconversion will usually test positive with the Western blot within one month of being tested during pregnancy or at delivery. The CDC recommends that all women in high risk areas (including Texas) be tested for HIV during the third trimester of pregnancy. (Effective January 1, 2010, Texas state law will change for HIV testing of pregnant women. Using an opt-out approach, an HIV test will be performed at the first prenatal care visit AND during the third trimester of pregnancy.)

C. Testing during Labor and Delivery

To reduce perinatal HIV transmission, the CDC recommends that rapid tests be administered to all women without a documented HIV status during labor. If the test results are positive, the woman should be given the appropriate antiretroviral prophylaxis immediately, rather than waiting for a confirmatory test. If a woman with an undocumented HIV status is not tested during labor, she should be tested immediately after delivery. The newborn should also have a rapid test as soon as possible. [1] (Effective January 1, 2010, Texas state law states if there is no record of a third trimester test when a woman arrives at labor and delivery, a test will be performed with laboratory results made available within 6 hours of submission of the sample. If there is no record of a third trimester test and no test was performed during labor and delivery, the infant must be tested within two hours of birth with results available within 6 hours of submission of the sample.)

5-7 Incidence and VARHS

BED-Capture Enzyme Immunoassay Used in the Serologic Testing Algorithm for Recent HIV Seroconversion (STARHS) Program

HIV incidence surveillance (HIS) is a recent a CDC-funded surveillance initiative aimed at producing estimates of the number of individuals newly infected with the HIV virus in a given year, including those undiagnosed. HIS utilizes new testing technology the Serologic Testing Algorithm for Recent HIV Seroconversion (*STARHS*) to classify HIV infections as likely or not likely to be recent (i.e., occurring within the past 6 months). STARHS testing is performed on confirmed HIV positive specimens using blood remaining after the HIV diagnostic test is completed. STARHS utilizes a new test developed by the CDC called the HIV-1 BED Capture EIA (BED) assay that is able to distinguish recent versus long-standing infections in persons with a confirmed positive test. This test measures the proportion of HIV-specific antibodies among all IgG antibodies in the serum (the level of these antibodies in the blood increases as the body

[1] Branson, et al. Revised Recommendations for HIV Testing of Adults, Adolescents, and Pregnant Women in Health-Care Settings. CDC. MMWR; 2006 55(RR14);1-17

responds to infection) to determine if an infection is recent or long-standing. The BED assay is approved by the Food and Drug Administration (FDA) for surveillance use only and is restricted from being used for diagnostic or clinical purposes. Because the BED assay has no clinical value for the individual patient, results are not be returned to the individual or the lab that conducts the initial EIA/Western blot.

HIV Resistance testing for VARHS

Variant Atypical and Resistant HIV surveillance (VARHS) is a CDC-funded surveillance initiative that incorporates the surveillance of transmitted strains of variant, atypical, and resistant HIV-1 into routine HIV surveillance activities. The purpose of VARHS is to evaluate the prevalence of HIV-1 drug resistance and the distribution of HIV-1 subtypes among persons with a new HIV diagnosis. HIV genetic sequencing is performed, by a CDC-contracted laboratory, on confirmed HIV positive specimens to detect the presence of mutations associated with antiretroviral drug resistance and HIV-1 subtypes. As part of the initiative, DSHS returns individual genotype results to care providers as designated by a patient with a signed release form. Due to project limitations, only specimens tested for HIV in publically funded laboratories are eligible for resistance testing through the VARHS project; specimens tested in commercial labs are not included.

Appendix A:
Revised Surveillance Case Definitions for HIV Infection Among Adults, Adolescents, and Children Aged <18 Months and for HIV Infection and AIDS Among Children Aged 18 Months to <13 Years — United States, 2008

CDC

MMWR™

Morbidity and Mortality Weekly Report

www.cdc.gov/mmwr

Recommendations and Reports December 5, 2008 / Vol. 57 / No. RR-10

Revised Surveillance Case Definitions for HIV Infection Among Adults, Adolescents, and Children Aged <18 Months and for HIV Infection and AIDS Among Children Aged 18 Months to <13 Years — United States, 2008

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR DISEASE CONTROL AND PREVENTION

The *MMWR* series of publications is published by the Coordinating Center for Health Information and Service, Centers for Disease Control and Prevention (CDC), U.S. Department of Health and Human Services, Atlanta, GA 30333.

Suggested Citation: Centers for Disease Control and Prevention. [Title]. MMWR 2008;57(No. RR-#):[inclusive page numbers].

Centers for Disease Control and Prevention

Julie L. Gerberding, MD, MPH
Director

Tanja Popovic, MD, PhD
Chief Science Officer

James W. Stephens, PhD
Associate Director for Science

Steven L. Solomon, MD
Director, Coordinating Center for Health Information and Service

Jay M. Bernhardt, PhD, MPH
Director, National Center for Health Marketing

Katherine L. Daniel, PhD
Deputy Director, National Center for Health Marketing

Editorial and Production Staff

Frederic E. Shaw, MD, JD
Editor, MMWR *Series*

Susan F. Davis, MD
(*Acting*) *Assistant Editor,* MMWR *Series*

Teresa F. Rutledge
Managing Editor, MMWR *Series*

David C. Johnson
(*Acting*) *Lead Technical Writer-Editor*

Catherine B. Lansdowne, MS
Project Editor

Martha F. Boyd
Lead Visual Information Specialist

Malbea A. LaPete
Stephen R. Spriggs
Visual Information Specialists

Kim L. Bright, MBA
Quang M. Doan, MBA
Phyllis H. King
Information Technology Specialists

Editorial Board

William L. Roper, MD, MPH, Chapel Hill, NC, Chairman
Virginia A. Caine, MD, Indianapolis, IN
David W. Fleming, MD, Seattle, WA
William E. Halperin, MD, DrPH, MPH, Newark, NJ
Margaret A. Hamburg, MD, Washington, DC
King K. Holmes, MD, PhD, Seattle, WA
Deborah Holtzman, PhD, Atlanta, GA
John K. Iglehart, Bethesda, MD
Dennis G. Maki, MD, Madison, WI
Sue Mallonee, MPH, Oklahoma City, OK
Patricia Quinlisk, MD, MPH, Des Moines, IA
Patrick L. Remington, MD, MPH, Madison, WI
Barbara K. Rimer, DrPH, Chapel Hill, NC
John V. Rullan, MD, MPH, San Juan, PR
William Schaffner, MD, Nashville, TN
Anne Schuchat, MD, Atlanta, GA
Dixie E. Snider, MD, MPH, Atlanta, GA
John W. Ward, MD, Atlanta, GA

CONTENTS

Introduction 1
Methods 1
Adults and Adolescents 1
Children 2
2008 Surveillance Case Definition for HIV Infection Among Adults and Adolescents 3
2008 Surveillance Case Definition for HIV Infection Among Children Aged <18 Months 5
2008 Surveillance Case Definitions for HIV Infection and AIDS Among Children Aged 18 Months to <13 Years 7
References 8
Appendices 9

Disclosure of Relationship

CDC, our planners, and our content experts wish to disclose they have no financial interests or other relationships with the manufacturers of commercial products, suppliers, or commercial services, or commercial supporters. Presentations will not include any discussion of the unlabeled use of a product or a product under investigational use.

Revised Surveillance Case Definitions for HIV Infection Among Adults, Adolescents, and Children Aged <18 Months and for HIV Infection and AIDS Among Children Aged 18 Months to <13 Years — United States, 2008

Prepared by
Eileen Schneider, MD
Suzanne Whitmore, DrPH
M. Kathleen Glynn, DVM
Kenneth Dominguez, MD
Andrew Mitsch, MPH
Matthew T. McKenna, MD
Division of HIV/AIDS Prevention, National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention

Summary

For adults and adolescents (i.e., persons aged ≥13 years), the human immunodeficiency virus (HIV) infection classification system and the surveillance case definitions for HIV infection and acquired immunodeficiency syndrome (AIDS) have been revised and combined into a single case definition for HIV infection (1–3). In addition, the HIV infection case definition for children aged <13 years and the AIDS case definition for children aged 18 months to <13 years have been revised (1,3,4). No changes have been made to the HIV infection classification system (4), the 24 AIDS-defining conditions (1,4) for children aged <13 years, or the AIDS case definition for children aged <18 months. These case definitions are intended for public health surveillance only and not as a guide for clinical diagnosis. Public health surveillance data are used primarily for monitoring the HIV epidemic and for planning on a population level, not for making clinical decisions for individual patients. CDC and the Council of State and Territorial Epidemiologists recommend that all states and territories conduct case surveillance of HIV infection and AIDS using the 2008 surveillance case definitions, effective immediately.

Introduction

Since the beginning of the human immunodeficiency virus (HIV) epidemic, case definitions for HIV infection and acquired immunodeficiency syndrome (AIDS) have undergone several revisions to respond to diagnostic and therapeutic advances and to improve standardization and comparability of surveillance data regarding persons at all stages of HIV disease. HIV testing is now widely available, and diagnostic testing has continued to improve; these changes are reflected in the 2008 revised case definition for HIV infection, which now requires laboratory-confirmed evidence of HIV infection to meet the case definition among adults, adolescents, and children aged 18 months to <13 years.

The material in this report originated in the National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention, Kevin Fenton, MD, PhD, Director; and the Division of HIV/AIDS Prevention, Richard Wolitski, PhD, Acting Director.
Corresponding preparer: Suzanne Whitmore, DrPH, National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention, 1600 Clifton Road, NE, MS E-47, Atlanta, GA 30333. Telephone: 404-639-1556; Fax: 404-639-2980; E-mail: swhitmore@cdc.gov.

Methods

CDC collaborated with the Council of State and Territorial Epidemiologists (CSTE) to develop the revisions in this report. CDC obtained additional input through consultations regarding the pediatric case definitions (April 2005) and adult and adolescent case definition (August 2005 and June 2006) and through peer review by health-care professionals, in compliance with the Office of Management and Budget requirements for the dissemination of influential scientific information.

Adults and Adolescents

For adults and adolescents (aged ≥13 years), the case definitions for HIV infection and AIDS have been revised into a single case definition for HIV infection that includes AIDS and incorporates the HIV infection classification system. Laboratory-confirmed evidence of HIV infection is now required to meet the surveillance case definition for HIV infection, including stage 3 HIV infection (AIDS). Diagnostic confirmation of an AIDS-defining condition alone (Appendix A), without laboratory-confirmed evidence of HIV infection, is no longer sufficient to classify an adult or adolescent as HIV

infected for surveillance purposes. The 2007 World Health Organization (WHO) revised surveillance case definition for HIV infection also requires laboratory confirmation of HIV infection (Appendix B).

Historically, the case definition for AIDS included adults and adolescents without laboratory-confirmed evidence of HIV infection if other clinical criteria were met. In 1993, the existing case definition for AIDS (*1*) was expanded to include 1) all HIV-infected persons with a CD4+ T-lymphocyte count of <200 cells/μL or a CD4+ T-lymphocyte percentage of total lymphocytes of <14 and 2) three additional clinical conditions (pulmonary tuberculosis, recurrent pneumonia, and invasive cervical cancer), in addition to retaining the 23 clinical conditions in the previous AIDS case definition (*2*). Despite these changes, the case definition for AIDS continued to include a subset of adults and adolescents without laboratory-confirmed evidence of HIV infection whose illness still met the surveillance case definition for AIDS. Illness in a person who did not have any other known cause of immunodeficiency met the surveillance case definition for AIDS if the illness met any of the following three criteria: 1) no laboratory testing performed or inconclusive laboratory evidence of HIV infection but a definitive diagnosis of a condition included in a subset of AIDS-defining conditions, 2) negative laboratory results for HIV infection but a definitive diagnosis of *Pneumocystis jirovecii* pneumonia, or 3) negative laboratory results for HIV infection but a definitive diagnosis of a condition included in a subset of AIDS-defining conditions and a CD4+ T-lymphocyte count of <400 cells/μL. Because of improvements in diagnostic capabilities and treatment, including increased use of new HIV-testing technologies, CDC collaborated with CSTE to recommend in 2005 an interim change in the AIDS case definition, which required laboratory confirmation of HIV infection. This recommended change required laboratory-confirmed evidence of HIV infection in addition to a CD4+ T-lymphocyte count of <200 cells/μL, a CD4+ T-lymphocyte percentage of total lymphocytes of <14, or diagnosis of an AIDS-defining condition (*5*). This CDC/CSTE interim recommendation has been incorporated into the 2008 HIV infection case definition, which includes AIDS (stage 3).

In 1993, the revised classification system for HIV infection and the expanded AIDS surveillance case definition for adults and adolescents were based on three clinical categories (i.e., A, B, and C) and three ranges of CD4+ T-lymphocyte counts (i.e., ≥500 cells/μL, 200–499 cells/μL, and <200 cells/μL) or the concordant CD4+ T-lymphocyte percentages (*2*). Clinical category A comprised asymptomatic acute or primary HIV infection or persistent generalized lymphadenopathy. Clinical category B comprised symptomatic conditions in an HIV-infected adult or adolescent that were not included in clinical categories A or C but were attributed to a cell-mediated immunity defect or for which the clinical course or management was complicated by HIV infection. Clinical category C comprised the 26 AIDS-defining conditions. In the context of treatment and diagnostic improvements since 1993, clinical categories A and B pose particular difficulties because they include many conditions that are not discrete diseases, are not necessarily indicators of immunodeficiency, poorly match current treatment guidelines, and are not integrated into routine surveillance practices. The classification system of the 2008 case definition for HIV infection, which includes AIDS, has been simplified, with less emphasis on clinical conditions by elimination of clinical categories A and B while retaining the 26 AIDS-defining conditions in clinical category C (*1,2*).

The role of CD4+ T-lymphocyte counts and percentages also has been clarified. The 2008 case definition highlights the central role of the CD4+ T-lymphocyte counts and percentages, which are objective measures of immunosuppression that are routinely used in the care of HIV-infected persons and are available to surveillance programs. The three CD4+ T-lymphocyte count categories have been renamed for HIV infection, increasing in severity from stage 1 through stage 3 (AIDS); an unknown stage also is included. For surveillance purposes, HIV disease progression is classified from less to more severe; once cases are classified into a surveillance severity stage, they cannot be reclassified into a less severe stage.

Children

Aged <18 Months

The 1999 surveillance guidelines recommended four categories of HIV infection for children aged <18 months: definitively HIV infected, presumptively HIV infected, definitively uninfected with HIV, and presumptively uninfected with HIV (*3*). Because of improved accuracy and the widespread availability of viral detection and antibody tests to diagnose HIV infection, changes have been made in the surveillance case definition of presumptively uninfected with HIV for children aged <18 months at the time of diagnosis (*1,3,4*). Thus, compared with infants categorized using the previous surveillance case definition, fewer HIV-exposed infants who have a very low probability of infection will be categorized as having indeterminate infections (*3*). No major revisions have been made to the remaining three categories for children aged <18 months, and no changes have been made to the AIDS surveillance case definition for children in this age group (*1,3,4*). Because of the greater uncertainty associated with diagnostic testing for HIV in this population (i.e., because maternal antibodies from the HIV-infected mother might exist in the infant after

birth, possibly affecting HIV diagnostic testing of the infant that occurs soon after birth), children in this age group whose illness meets clinical criteria for the AIDS case definition but does not meet laboratory criteria for definitive or presumptive HIV infection are still categorized as HIV infected when the mother has laboratory-confirmed HIV infection.

Aged 18 Months to <13 Years

For children aged 18 months to <13 years, laboratory-confirmed evidence of HIV infection is now required to meet the surveillance case definition for HIV infection and AIDS. Diagnostic confirmation of an AIDS-defining condition alone, without laboratory-confirmed evidence of HIV infection, is no longer sufficient to classify a child as HIV infected for surveillance purposes (*1,3,4*). No changes have been made to the 24 AIDS-defining conditions (*1,4*) or the HIV infection classification system for children aged <13 years (*4*).

2008 Surveillance Case Definition for HIV Infection Among Adults and Adolescents

The 2008 HIV infection case definition for adults and adolescents (aged ≥13 years) replaces the HIV infection and AIDS case definitions and the HIV infection classification system (*1–3,5*). The case definition is intended for public health surveillance only and not as a guide for clinical diagnosis. The definition applies to all HIV variants (e.g., HIV-1 or HIV-2) and excludes confirmation of HIV infection through diagnosis of AIDS-defining conditions alone. For surveillance purposes, a reportable case of HIV infection among adults and adolescents aged ≥13 years is categorized by increasing severity as stage 1, stage 2, or stage 3 (AIDS) or as stage unknown (Table).

Criteria for HIV Infection

Laboratory Criteria

- Positive result from an HIV antibody screening test (e.g., reactive enzyme immunoassay [EIA]*) confirmed by a positive result from a supplemental HIV antibody test (e.g., Western blot or indirect immunofluorescence assay test).

or

- Positive result or report of a detectable quantity (i.e., within the established limits of the laboratory test) from any of the following HIV virologic (i.e., non-antibody) tests†:
  - — HIV nucleic acid (DNA or RNA) detection test (e.g., polymerase chain reaction [PCR])
  - — HIV p24 antigen test, including neutralization assay
  - — HIV isolation (viral culture)

Other Criterion (for Cases that Do Not Meet Laboratory Criteria)

- HIV infection diagnosed by a physician or qualified medical-care provider§ based on the laboratory criteria and documented in a medical record.¶ Oral reports of prior laboratory test results are not acceptable.

Case Classification

A confirmed case meets the laboratory criteria for diagnosis of HIV infection and one of the four HIV infection stages (stage 1, stage 2, stage 3, or stage unknown) (Table). Although cases with no information on CD4+ T-lymphocyte count or percentage and no information on AIDS-defining conditions can be classified as stage unknown, every effort should be made to report CD4+ T-lymphocyte counts or percentages and the presence of AIDS-defining conditions at the time of diagnosis. Additional CD4+ T-lymphocyte counts or percentages and any identified AIDS-defining conditions can be reported as recommended (*6*).

HIV Infection, Stage 1

- No AIDS-defining condition and either CD4+ T-lymphocyte count of ≥500 cells/μL or CD4+ T-lymphocyte percentage of total lymphocytes of ≥29.

HIV Infection, Stage 2

- No AIDS-defining condition and either CD4+ T-lymphocyte count of 200–499 cells/μL or CD4+ T-lymphocyte percentage of total lymphocytes of 14–28.

* Rapid tests are EIAs that do not have to be repeated but require a confirmatory test if reactive. Most conventional EIAs require a repeatedly reactive EIA that is confirmed by a positive result with a supplemental test for HIV antibody. Standard laboratory testing procedures should always be followed.

† For HIV screening, HIV virologic (non-antibody) tests should not be used in lieu of approved HIV antibody screening tests. A negative result (i.e., undetectable or nonreactive) from an HIV virologic test (e.g., viral RNA nucleic acid test) does not rule out the diagnosis of HIV infection.

§ Qualified medical-care providers might differ by jurisdiction and might include physicians, nurse practitioners, physician assistants, or nurse midwives.

¶ An original or copy of the laboratory report is preferred; however, in the rare instance the laboratory report is not available, a description of the laboratory report results by a physician or qualified medical-care provider documented in the medical record is acceptable for surveillance purposes. Every effort should be made to obtain a copy of the laboratory report for documentation in the medical record.

TABLE. Surveillance case definition for human immunodeficiency virus (HIV) infection among adults and adolescents (aged ≥13 years) — United States, 2008

Stage	Laboratory evidence*	Clinical evidence
Stage 1	Laboratory confirmation of HIV infection *and* CD4+ T-lymphocyte count of ≥500 cells/μL *or* CD4+ T-lymphocyte percentage of ≥29	None required (but no AIDS-defining condition)
Stage 2	Laboratory confirmation of HIV infection *and* CD4+ T-lymphocyte count of 200–499 cells/μL *or* CD4+ T-lymphocyte percentage of 14–28	None required (but no AIDS-defining condition)
Stage 3 (AIDS)	Laboratory confirmation of HIV infection *and* CD4+ T-lymphocyte count of <200 cells/μL *or* CD4+ T-lymphocyte percentage of <14†	*or* documentation of an AIDS-defining condition (with laboratory confirmation of HIV infection)†
Stage unknown§	Laboratory confirmation of HIV infection *and* no information on CD4+ T-lymphocyte count or percentage	*and* no information on presence of AIDS-defining conditions

* The CD4+ T-lymphocyte percentage is the percentage of total lymphocytes. If the CD4+ T-lymphocyte count and percentage do not correspond to the same HIV infection stage, select the more severe stage.

† Documentation of an AIDS-defining condition (Appendix A) supersedes a CD4+ T-lymphocyte count of ≥200 cells/μL and a CD4+ T-lymphocyte percentage of total lymphocytes of ≥14. Definitive diagnostic methods for these conditions are available in Appendix C of the 1993 revised HIV classification system and the expanded AIDS case definition (CDC. 1993 Revised classification system for HIV infection and expanded surveillance case definition for AIDS among adolescents and adults. MMWR 1992;41[No. RR-17]) and from the National Notifiable Diseases Surveillance System (available at http://www.cdc.gov/epo/dphsi/casedef/case_definitions.htm).

§ Although cases with no information on CD4+ T-lymphocyte count or percentage or on the presence of AIDS-defining conditions can be classified as stage unknown, every effort should be made to report CD4+ T-lymphocyte counts or percentages and the presence of AIDS-defining conditions at the time of diagnosis. Additional CD4+ T-lymphocyte counts or percentages and any identified AIDS-defining conditions can be reported as recommended. (Council of State and Territorial Epidemiologists. Laboratory reporting of clinical test results indicative of HIV infection: new standards for a new era of surveillance and prevention [Position Statement 04-ID-07]; 2004. Available at http://www.cste.org/ps/2004pdf/04-ID-07-final.pdf.)

HIV Infection, Stage 3 (AIDS)

- CD4+ T-lymphocyte count of <200 cells/μL or CD4+ T-lymphocyte percentage of total lymphocytes of <14 or documentation of an AIDS-defining condition (Appendix A). Documentation of an AIDS-defining condition supersedes a CD4+ T-lymphocyte count of ≥200 cells/μL and a CD4+ T-lymphocyte percentage of total lymphocytes of ≥14. Definitive diagnostic methods for these conditions are available in Appendix C of the 1993 revised HIV classification system and the expanded AIDS case definition (*2*) and from the National Notifiable Diseases Surveillance System (available at http://www.cdc.gov/epo/dphsi/casedef/case_definitions.htm).

HIV Infection, Stage Unknown

- No information available on CD4+ T-lymphocyte count or percentage and no information available on AIDS-defining conditions. (Every effort should be made to report CD4+ T-lymphocyte counts or percentages and the presence of AIDS-defining conditions at the time of diagnosis.)

Discussion

To meet the surveillance case definition for HIV infection among adults and adolescents, laboratory-confirmed evidence of HIV infection is required. The lowest CD4+ T-lymphocyte count (or concordant CD4+ T-lymphocyte percentage of total lymphocytes) or the presence of AIDS-defining conditions is used to determine the stage of infection. If the CD4+ T-lymphocyte count and the CD4+ T-lymphocyte percentage are both available but do not correspond to the same severity stage, select the more severe stage. For surveillance purposes, disease progression is from less to more severe; once cases are classified in a more severe surveillance stage, they cannot be reclassified into a less severe surveillance stage.

A diagnosis of acute HIV infection indicates documented evidence of detectable HIV RNA or DNA or of p24 antigen in plasma or serum in the presence of a documented negative or indeterminate result from an HIV antibody test. These laboratory tests should be conducted on the same specimen or on specimens obtained on the same day. Acute HIV infection occurs approximately during the time from viral acquisition until seroconversion (i.e., the development of measurable levels of HIV-specific antibodies). During this period, early immune responses to the virus produce distinctive characteristics; 40% to 80% of patients develop clinical symptoms of a nonspecific viral illness (e.g., fever, fatigue, or rash) typically lasting 1–2 weeks (*7–12*). Acute HIV infection often is not detected because the date of HIV acquisition is unknown, no specific clinical signs are present, no single laboratory marker is present, and the diagnostic window is small. High viral loads typically are associated with acute HIV infection, potentially increasing the risk for transmission. CD4+ T-lymphocyte counts have decreased in certain patients with acute HIV

infection, especially during the months immediately following viral acquisition (*7,11,12*). However, the viral load and CD4+ T-lymphocyte count usually stabilize once equilibrium is reached between HIV and the immune response (i.e., the viral set point). The changing CD4+ T-lymphocyte counts associated with acute HIV infection might have implications when using these counts to stage HIV infection for surveillance purposes; for example, persons might experience a particularly low, but temporary, CD4+ T-lymphocyte count and be categorized as having a more severe stage of HIV infection than they actually have after reaching the viral set point.

2008 Surveillance Case Definition for HIV Infection Among Children Aged <18 Months

The 2008 case definition of HIV infection among children aged <18 months replaces the definition published in 1999 (*3*) and applies to all variants of HIV (e.g., HIV-1 or HIV-2). The 2008 definition is intended for public health surveillance only and not as a guide for clinical diagnosis.

The 2008 definition takes into account new available testing technologies. Laboratory criteria for children aged <18 months at the time of diagnosis include revisions to one category: presumptively uninfected with HIV. No substantial changes have been made to the remaining three categories (definitively HIV infected, presumptively HIV infected, and definitively uninfected with HIV), and no changes have been made to the conditions listed under the AIDS criteria in the 1987 pediatric surveillance case definition for AIDS for children aged <18 months (*1,3,13*). Because diagnostic laboratory testing for HIV infection among children aged <18 months might be unreliable, children in this age group with perinatal HIV exposure whose illness meets the AIDS case definition on the basis of clinical criteria are considered presumptively HIV infected when the mother has laboratory-confirmed HIV infection. The definitive or presumptive exclusion of HIV infection for surveillance purposes does not mean that clinical HIV infection can be ruled out. For the purposes of calculating the exact timing of tests (e.g., when a specimen was obtained for laboratory testing) based on the surveillance case definition, 1 month corresponds to 30 days.

Criteria for Definitive or Presumptive HIV Infection

A child aged <18 months is categorized for surveillance purposes as definitively or presumptively HIV infected if born to an HIV-infected mother and if the laboratory criterion or at least one of the other criteria is met.

Laboratory Criterion for Definitive HIV Infection

A child aged <18 months is categorized for surveillance purposes as definitively HIV infected if born to an HIV-infected mother and the following laboratory criterion is met.

- Positive results on two separate specimens (not including cord blood) from one or more of the following HIV virologic (non-antibody) tests:
  - HIV nucleic acid (DNA or RNA) detection**
  - HIV p24 antigen test, including neutralization assay, for a child aged ≥1 month
  - HIV isolation (viral culture)

Laboratory Criterion for Presumptive HIV Infection

A child aged <18 months is categorized for surveillance purposes as presumptively HIV infected if 1) born to an HIV-infected mother, 2) the criterion for definitively HIV infected is not met, and 3) the following laboratory criterion is met.

- Positive results on one specimen (not including cord blood) from the listed HIV virologic tests (HIV nucleic acid detection test; HIV p24 antigen test, including neutralization assay, for a child aged ≥1 month; or HIV isolation [viral culture] for definitively HIV infected) and no subsequent negative results from HIV virologic or HIV antibody tests.

Other Criteria (for Cases that Do Not Meet Laboratory Criteria for Definitive or Presumptive HIV Infection)

- HIV infection diagnosed by a physician or qualified medical-care provider based on the laboratory criteria and documented in a medical record. Oral reports of prior laboratory test results are not acceptable.

or

** HIV nucleic acid (DNA or RNA) detection tests are the virologic methods of choice for the diagnosis or exclusion of infection in children aged <18 months. Although HIV culture can be used, culture is less standardized and less sensitive than nucleic acid detection tests. The use of p24 antigen testing to exclude infection in children aged <18 months is not recommended because of poor sensitivity, especially in the presence of HIV antibody. Commercial tests for RNA and DNA detection have become widely available. Quantitative RNA tests have been approved by the Food and Drug Administration (FDA) for monitoring HIV infection, and qualitative RNA tests have been approved to aid diagnosis. The quantitative and qualitative RNA tests meet FDA standards for high analytic and clinical sensitivity and specificity (*14–16*). All available tests detect the subtypes of group M and strains of group O. HIV-2 can be diagnosed with HIV-2 DNA PCR. HIV RNA tests sometimes do not detect HIV-2 because the viral loads in some HIV-2–infected persons are below detectable levels. Because of the possibility of mutation or recombination involving the sequences detected by a particular test, occasionally, virus might not be detected in a specimen from an HIV-2 infected individual. If HIV-2 infection seems likely but results are negative, testing with a different assay might be advisable.

- When test results regarding HIV infection status are not available, documentation of a condition that meets the criteria in the 1987 pediatric surveillance case definition for AIDS (*1*) (Appendix A).

Criteria for Uninfected with HIV, Definitive or Presumptive

A child aged <18 months born to an HIV-infected mother is categorized for surveillance purposes as either definitively or presumptively uninfected with HIV if 1) the criteria for definitive or presumptive HIV infection are not met and 2) at least one of the laboratory criteria or other criteria are met.

Laboratory Criteria for Uninfected with HIV, Definitive

A child aged <18 months born to an HIV-infected mother is categorized for surveillance purposes as definitively uninfected with HIV if 1) the criteria for definitive or presumptive HIV infection are not met and 2) at least one of the laboratory criteria or other criteria are met.[††]

- At least two negative HIV DNA or RNA virologic tests from separate specimens, both of which were obtained at age ≥1 month and one of which was obtained at age ≥4 months.

or

- At least two negative HIV antibody tests from separate specimens obtained at age ≥6 months.

and

- No other laboratory or clinical evidence of HIV infection (i.e., no positive results from virologic tests [if tests were performed] and no current or previous AIDS-defining condition) (Appendix A).

Laboratory Criteria for Uninfected with HIV, Presumptive

A child aged <18 months born to an HIV-infected mother is categorized for surveillance purposes as presumptively uninfected with HIV if 1) the criteria for definitively uninfected with HIV are not met and 2) at least one of the laboratory criteria are met.

- Two negative RNA or DNA virologic tests, from separate specimens, both of which were obtained at age ≥2 weeks and one of which was obtained at age ≥4 weeks.[§§]

or

- One negative RNA or a DNA virologic test from a specimen obtained at age ≥8 weeks.

or

- One negative HIV antibody test from a specimen obtained at age ≥6 months.

or

- One positive HIV virologic test followed by at least two negative tests from separate specimens, one of which is a virologic test from a specimen obtained at age ≥8 weeks or an HIV antibody test from a specimen obtained at age ≥6 months.

and

- No other laboratory or clinical evidence of HIV infection (i.e., no subsequent positive results from virologic tests if tests were performed, and no AIDS-defining condition for which no other underlying condition indicative of immunosuppression exists) (Appendix A).

Other Criteria (for Cases that Do Not Meet Laboratory Criteria for Uninfected with HIV, Definitive or Presumptive)

- Determination of uninfected with HIV by a physician or qualified medical-care provider based on the laboratory criteria and who has noted the HIV diagnostic test results in the medical record. Oral reports of prior laboratory test results are not acceptable.

and

- No other laboratory or clinical evidence of HIV infection (i.e., no positive results from virologic tests [if tests were performed] and no AIDS-defining condition for which no other underlying condition indicative of immunosuppression exists) (Appendix A).

Criteria for Indeterminate HIV Infection

A child aged <18 months born to an HIV-infected mother is categorized as having perinatal exposure with an indeterminate HIV infection status if the criteria for infected with HIV and uninfected with HIV are not met.

Discussion

The exclusion of HIV infection (definitive or presumptive) for surveillance purposes does not mean that clinical HIV infection can be ruled out. These categories are used for surveillance classification purposes and should not be used to guide clinical practice. A child with perinatal HIV exposure should continue to be monitored clinically according to nationally accepted treatment and care guidelines (*17–19*) to 1) monitor for potential complications of exposure to antiretroviral medications during

[††] Suspected cases of HIV infection among children aged <18 months who are born to a documented HIV-uninfected mother should be assessed on a case-by-case basis by the appropriate health care and public health specialists.

[§§] If specimens for both negative RNA or DNA virologic tests are obtained at age ≥4 weeks, specimens should be obtained on separate days.

the perinatal period and 2) confirm the absence of HIV infection with repeat clinical and laboratory evaluations.

No changes have been made to the existing classification system for HIV infection among children aged <18 months (*4*). To classify HIV-infected children in this age group, use the 1994 revised classification system for HIV infection among children aged <13 years (*4*).

2008 Surveillance Case Definitions for HIV Infection and AIDS Among Children Aged 18 Months to <13 Years

These 2008 surveillance case definitions of HIV infection and AIDS supersede those published in 1987 (*1*) and 1999 (*3*) and apply to all variants of HIV (e.g., HIV-1 or HIV-2). They are intended for public health surveillance only and are not a guide for clinical diagnosis.

The 2008 laboratory criteria for reportable HIV infection among persons aged 18 months to <13 years exclude confirmation of HIV infection through the diagnosis of AIDS-defining conditions alone. Laboratory-confirmed evidence of HIV infection is now required for all reported cases of HIV infection among children aged 18 months to <13 years (*20*).

Criteria for HIV Infection

Children aged 18 months to <13 years are categorized as HIV infected for surveillance purposes if at least one of laboratory criteria or the other criterion is met.¶¶

Laboratory Criteria

- Positive result from a screening test for HIV antibody (e.g., reactive EIA), confirmed by a positive result from a supplemental test for HIV antibody (e.g., Western blot or indirect immunofluorescence assay).

or

- Positive result or a detectable quantity by any of the following HIV virologic (non-antibody) tests***:
  — HIV nucleic acid (DNA or RNA) detection (e.g., PCR)
  — HIV p24 antigen test, including neutralization assay
  — HIV isolation (viral culture)

¶¶ Children aged 18 months to <13 years with perinatal exposure to HIV are categorized as uninfected with HIV if the criteria for uninfected with HIV among children aged <18 months are met.

*** For HIV screening among children aged 18 months to <13 years infected through exposure other than perinatal exposure, HIV virologic (non-antibody) tests should not be used in lieu of approved HIV antibody screening tests. A negative result (i.e., undetectable or nonreactive) by an HIV virologic test (e.g., viral RNA nucleic acid test) does not rule out the diagnosis of HIV infection.

Other Criterion (for Cases that Do Not Meet Laboratory Criteria)

- HIV infection diagnosed by a physician or qualified medical-care provider based on the laboratory criteria and documented in a medical record. Oral reports of prior laboratory test results are not acceptable.

Criteria for AIDS

Children aged 18 months to <13 years are categorized for surveillance purposes as having AIDS if the criteria for HIV infection are met and at least one of the AIDS-defining conditions has been documented (Appendix A).

The 2008 surveillance case definition for AIDS retains the 24 clinical conditions in the AIDS surveillance case definition published in 1987 (*1*) and revised in 1994 (*4*) for children aged <13 years (Appendix A). Because the 2008 definition requires that all AIDS diagnoses have laboratory-confirmed evidence of HIV infection, the presence of any AIDS-defining condition listed in Appendix A indicates a surveillance diagnosis of AIDS. Guidance on the diagnosis of these diseases in the context of all nationally notifiable diseases is available at http://www.cdc.gov/epo/dphsi/casedef/case_definitions.htm.

Discussion

To meet the surveillance case definition for HIV infection, laboratory confirmation of HIV infection is now required for children aged 18 months to <13 years. To meet the surveillance case definition for AIDS, in addition to the presence of one or more AIDS-defining conditions, laboratory-confirmed evidence of HIV infection is now required for children aged 18 months to <13 years. These revisions will increase the specificity of the HIV infection and AIDS surveillance case definitions by excluding patients without laboratory-confirmed evidence of HIV infection, reinforcing the public health message that HIV infection is the cause of AIDS. Improved specificity will provide more accurate data regarding number of HIV infection cases, which can be used to refine public health policies and determine appropriate use of HIV resources.

No changes have been made to the existing classification system for HIV infection among children aged 18 months to <13 years (*4*). To classify HIV-infected children in this age group, refer to the 1994 revised classification system for HIV infection among children aged <13 years (*4*).

Acknowledgments

This report is based, in part, on contributions by Bernard Branson, MD, Tonji Durant, PhD, Mary Glenn Fowler, MD, Lisa M. Lee, PhD, Kathleen McDavid Harrison, PhD, Nan Ruffo, Richard Selik, MD, Division of HIV/AIDS Prevention, Irum Zaidi, MPH, Keith

Sabin, PhD, Theresa Diaz, MD, Division of Global AIDS, National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention, Christine L. Mattson, PhD, EIS Officer, CDC; Stephanie Broyles, PhD, Pennington Biomedical Research Center, Baton Rouge, Louisiana; Victoria Cargill, MD, National Institutes of Health, Rockville, Maryland; Laura Cheever, MD, Health Resources and Services Administration, Rockville, Maryland; Peter Havens, MD, Medical College of Wisconsin and Children's Hospital of Wisconsin, Milwaukee, Wisconsin; Ellen Moore, MD, Wayne State University School of Medicine, Detroit, Michigan; Pauline Thomas, MD, University of Medicine and Dentistry of New Jersey, Newark, New Jersey; and Jesus Maria Garcia Calleja, MD, World Health Organization, Geneva, Switzerland.

References

1. CDC. Revision of the CDC surveillance case definition for acquired immunodeficiency syndrome. MMWR 1987;36(Suppl 1):1–15.
2. CDC. 1993 Revised classification system for HIV infection and expanded surveillance case definition for AIDS among adolescents and adults. MMWR 1992;41(No. RR-17).
3. CDC. Guidelines for national human immunodeficiency virus case surveillance, including monitoring for human immunodeficiency virus infection and acquired immunodeficiency syndrome. MMWR 1999;48(No. RR-13).
4. CDC. 1994 Revised classification system for human immunodeficiency virus infection in children less than 13 years of age. MMWR 1994; 43(No. RR-12).
5. Council of State and Territorial Epidemiologists. Revision of surveillance case definition for AIDS among adults and adolescents ≥13 years of age (Position Statement 05-ID-04); 2005. Available at http://www.cste.org/ps/2005pdf/final2005/05-ID-04final.pdf.
6. Council of State and Territorial Epidemiologists. Laboratory reporting of clinical test results indicative of HIV infection: new standards for a new era of surveillance and prevention (Position Statement 04-ID-07); 2004. Available at http://www.cste.org/ps/2004pdf/04-ID-07-final.pdf.
7. Kahn JO, Walker BD. Acute human immunodeficiency virus type 1 infection. N Engl J Med 1998;339:33–9.
8. Pilcher CD, Eron JJ Jr, Galvin S, Gay C, Cohen MS. Acute HIV revisited: new opportunities for treatment and prevention. J Clin Invest 2004;113:937–45. Erratum in: J Clin Invest 2006;116:3292.
9. Soogoor M, Daar ES. Primary human immunodeficiency virus type 1 infection. Curr HIV/AIDS Rep 2005;2:55–60.
10. Stekler J, Collier AC. Primary HIV infection. Curr HIV/AIDS Rep 2004; 1:68–73.
11. Schacker TW, Hughes JP, Shea T, Coombs RW, Corey L. Biological and virologic characteristics of primary HIV infection. Ann Intern Med 1998;128:613–20.
12. Zetola NM, Pilcher CD. Diagnosis and management of acute HIV infection. Infect Dis Clin North Am 2007;21:19–48.
13. Council of State and Territorial Epidemiologists. Revision of surveillance case definition for HIV infection among children aged <18 months (Position Statement 07-ID-10); 2007. Available at http://www.cste.org/PS/2007ps/2007psfinal/ID/07-ID-10.pdf.
14. Peter JB, Sevall JS. Molecular-based methods for quantifying HIV viral load. AIDS Patient Care STDs 2004;18:75–9.
15. Lelie PN, van Drimmelen HA, Cuypers HT, et al. Sensitivity of HCV RNA and HIV RNA blood screening assays. Transfusion 2002;42: 527–36.
16. Gallarda JL, Dragon E. Blood screening by nucleic acid amplification technology: current issues, future challenges. Mol Diagn 2000;5:11–22.
17. Working Group on Antiretroviral Therapy and Medical Management of HIV-Infected Children. Guidelines for the use of antiretroviral agents in pediatric HIV infection; 2008. Available at http://aidsinfo.nih.gov/contentfiles/pediatricguidelines.pdf.
18. Perinatal HIV Guidelines Working Group; Public Health Service Task Force. Recommendations for use of antiretroviral drugs in pregnant HIV-infected women for maternal health and interventions to reduce perinatal HIV transmission in the United States; 2008. Available at http://aidsinfo.nih.gov/contentfiles/perinatalgl.pdf.
19. King SM, Committee on Pediatric AIDS (American Academy of Pediatrics), Infectious Diseases and Immunization Committee (Canadian Paediatric Society). Evaluation and treatment of the human immunodeficiency virus-1–exposed infant. Pediatrics 2004;114:497–505.
20. Council of State and Territorial Epidemiologists. Revision of surveillance case definition for HIV infection and AIDS among children aged ≥18 months but <13 years (Position Statement 06-ID-02). June 2006. Available at http://www.cste.org/ps/2006pdfs/psfinal2006/06-id-02final.pdf.

Appendix A
AIDS-Defining Conditions

- Bacterial infections, multiple or recurrent*
- Candidiasis of bronchi, trachea, or lungs
- Candidiasis of esophagus†
- Cervical cancer, invasive§
- Coccidioidomycosis, disseminated or extrapulmonary
- Cryptococcosis, extrapulmonary
- Cryptosporidiosis, chronic intestinal (>1 month's duration)
- Cytomegalovirus disease (other than liver, spleen, or nodes), onset at age >1 month
- Cytomegalovirus retinitis (with loss of vision)†
- Encephalopathy, HIV related
- Herpes simplex: chronic ulcers (>1 month's duration) or bronchitis, pneumonitis, or esophagitis (onset at age >1 month)
- Histoplasmosis, disseminated or extrapulmonary
- Isosporiasis, chronic intestinal (>1 month's duration)
- Kaposi sarcoma†
- Lymphoid interstitial pneumonia or pulmonary lymphoid hyperplasia complex*†
- Lymphoma, Burkitt (or equivalent term)
- Lymphoma, immunoblastic (or equivalent term)
- Lymphoma, primary, of brain
- *Mycobacterium avium* complex or *Mycobacterium kansasii,* disseminated or extrapulmonary†
- *Mycobacterium tuberculosis* of any site, pulmonary,†§ disseminated,† or extrapulmonary†
- *Mycobacterium*, other species or unidentified species, disseminated† or extrapulmonary†
- *Pneumocystis jirovecii* pneumonia†
- Pneumonia, recurrent†§
- Progressive multifocal leukoencephalopathy
- *Salmonella* septicemia, recurrent
- Toxoplasmosis of brain, onset at age >1 month†
- Wasting syndrome attributed to HIV

* Only among children aged <13 years. (CDC. 1994 Revised classification system for human immunodeficiency virus infection in children less than 13 years of age. MMWR 1994;43[No. RR-12].)
† Condition that might be diagnosed presumptively.
§ Only among adults and adolescents aged ≥13 years. (CDC. 1993 Revised classification system for HIV infection and expanded surveillance case definition for AIDS among adolescents and adults. MMWR 1992;41[No. RR-17].)

Appendix B

Comparison of the Revised World Health Organization and CDC Surveillance Case Definitions and Staging Systems for HIV Infection

In 2007, the World Health Organization (WHO) revised the standard human immunodeficiency virus (HIV) infection and acquired immunodeficiency syndrome (AIDS) clinical staging system and the clinical and surveillance case definitions (*1*). The definitions were revised to 1) provide standardized HIV infection and AIDS surveillance case definitions, 2) simplify clinical staging, 3) coordinate the WHO 2002 three-stage pediatric staging system with the WHO 1990 four-stage adult system, 4) include immunologic criteria and clinical staging in case definitions, and 5) coordinate the clinical staging and surveillance case definitions. This appendix summarizes the revised criteria for WHO case surveillance and compares the 2007 revised WHO definitions with the 2008 revised CDC definitions. Despite differences in WHO and CDC disease classification and staging and because CDC recommends reporting all CD4+ T-lymphocyte counts for persons, the revised WHO case definition still allows comparison of CDC surveillance data from the United States with WHO data from other countries.

Revised WHO Definitions

Surveillance Case Definitions

WHO recommends reporting cases of HIV infection as HIV infection or advanced HIV disease (AHD), including AIDS. All cases of HIV infection, AHD, and AIDS require a confirmed diagnosis of HIV infection based on laboratory testing, using the appropriate national testing algorithm (*1*). The revised WHO surveillance case definitions include the following: HIV infection (stages 1 and 2), AHD (stage 3), and AIDS (stage 4) (*1*).

Clinical Staging and Immunologic Criteria

Four clinical stages have been established for persons with confirmed HIV infection. These stages include the full spectrum of HIV infection and coincide with WHO clinical treatment recommendations: 1) no symptoms, 2) mild symptoms, 3) advanced symptoms, and 4) severe symptoms (*1*). The revised staging systems include presumptive clinical diagnoses that can be made in the absence of laboratory tests and definitive clinical criteria that require confirmatory laboratory tests. The clinical stage provides useful information when HIV infection is first diagnosed, when a person begins receiving care for HIV infection, for tracking patients in treatment programs, and to guide decisions on when to initiate cotrimoxazole prophylaxis and antiretroviral therapy (ART).

Age-specific immunologic criteria for the disease classification are presented. For children aged <5 years, the CD4+ T-lymphocyte percentage of total lymphocytes rather than the absolute CD4+ T-lymphocyte count should be used because the absolute count tends to vary, more than the percentage, per individual child in this age group. Immunologic and clinical criteria should be documented (when available) to describe a case of HIV infection.

Comparison of the WHO and CDC Definitions

Both the WHO and CDC surveillance case definitions for HIV infection now require laboratory confirmation of HIV infection. Differences between the WHO and CDC definitions and staging systems include the following (Table):

1. WHO recommends reporting cases of HIV infection as HIV infection or AHD (including AIDS), whereas CDC recommends reporting cases of HIV infection by stage (i.e., stage 1, stage 2, stage 3, or stage unknown).
2. WHO presents four clinical stages for disease classification to reflect the WHO ART treatment guidelines, whereas CDC presents three, combining WHO stages 2 and 3 into CDC stage 2.
3. Because of increased, although not universal, availability of CD4+ T-lymphocyte testing, WHO recommends using clinical and immunologic criteria for clinical staging. CDC recommends using only immunologic criteria for staging, with the exception of stage 3, for which cases must have a CD4+ T-lymphocyte count of <200 cells/μL or a CD4+ T-lymphocyte percentage of <14 or one of 26 AIDS-defining conditions.

Despite these differences in disease classification and clinical staging and because CDC recommends reporting all CD4+ T-lymphocyte counts, CDC and WHO stages can still be compared.

Reference

1. World Health Organization (WHO). WHO case definitions of HIV for surveillance and revised clinical staging and immunological classification of HIV-related disease in adults and children. Geneva, Switzerland: WHO Press; 2007. Available at http://www.who.int/hiv/pub/guidelines/hivstaging/en/index.html.

TABLE. Comparison of World Health Organization (WHO) and CDC stages of human immunodeficiency virus (HIV) infection,* by CD4+ T-lymphocyte count and percentage of total lymphocytes

WHO stage†	WHO T-lymphocyte count and percentage§	CDC stage¶	CDC T-lymphocyte count and percentage
Stage 1 (HIV infection)	CD4+ T-lymphocyte count of ≥500 cells/μL	Stage 1 (HIV infection)	CD4+ T-lymphocyte count of ≥500 cells/μL *or* CD4+ T-lymphocyte percentage of ≥29
Stage 2 (HIV infection)	CD4+ T-lymphocyte count of 350–499 cells/μL	Stage 2 (HIV infection)	CD4+ T-lymphocyte count of 200–499 cells/μL *or* CD4+ T-lymphocyte percentage of 14–28
Stage 3 (advanced HIV disease [AHD])	CD4+ T-lymphocyte count of 200–349 cells/μL	Stage 2 (HIV infection)	CD4+ T-lymphocyte count of 200–499 cells/μL *or* CD4+ T-lymphocyte percentage of 14–28
Stage 4 (acquired immunodeficiency syndrome [AIDS])	CD4+ T-lymphocyte count of <200 cells/μL *or* CD4+ T-lymphocyte percentage of <15	Stage 3 (AIDS)	CD4+ T-lymphocyte count of <200 cells/μL *or* CD4+ T-lymphocyte percentage of <14

* For reporting purposes only.
† Among adults and children aged ≥5 years.
§ Percentage applicable for stage 4 only.
¶ Among adults and adolescents (aged ≥13 years). CDC also includes a fourth stage, stage unknown: laboratory confirmation of HIV infection but no information on CD4+ T-lymphocyte count or percentage *and* no information on AIDS-defining conditions.

CDC Adult/Adolescent HIV/AIDS Surveillance Case Definition Consultation, August 2005

External Consultants: Kathryn Anastos, MD, Montefiore Medical Center, Bronx, New York; Chris Archibald, MDCM, Public Health Agency of Canada, Ottawa, Ontario, Canada; John Barnhart, National Alliance of State and Territorial AIDS Directors, Washington, DC; Samuel A. Bozzette, MD, PhD, RAND Corporation, Santa Monica, California; Txema Calleja, MD, World Health Organization, Geneva, Switzerland; Charles C.J. Carpenter, MD, University Medicine Foundation, Inc., Providence, Rhode Island; Siobhan Crowley, MB, MRCP, World Health Organization, Geneva, Switzerland; Richard Davey, MD, National Institues of Health, Bethesda, Maryland; Eric A. Engels, MD, National Institutes of Health, Rockville, Maryland; Douglas Frye, MD, Los Angeles County HIV Epidemiology Program, Los Angeles, California; Donna Futterman, MD, Children's Hospital at Montefiore, Bronx, New York; Becky Grigg, Florida Department of Health, Tallahassee, Florida; Françoise Hamers, EuroHIV, Saint Maurice Cedex, France; W. Claire Hicks, MD, Georgia Department of Public Health, Jesup, Georgia; Scott Holmberg, MD, Research Triangle Institute (RTI) International, Atlanta, Georgia; Jack Jourden, MPH, Washington State Department of Health, Olympia, Washington; Alice Kroliczak, PhD, Health Resources and Services Adminstration, Rockville, Maryland; Alan Lifson, MD, University of Minnesota, Minneapolis, Minnesota; Norman Markowitz, MD, The Community Program for Clinical Research on AIDS, Henry Ford Health System, Detroit, Michigan; Anthony Merriweather, Alabama Department of Public Health, Montgomery, Alabama; Frank J. Palella, MD, Northwestern University Medical School, Chicago, Illinois; Jennifer Pennock, MSc, Public Health Agency of Canada, Ottawa, Ontario, Canada; Timothy R. Sterling, MD, Vanderbilt University Medical Center, Nashville, Tenessee; Karen T. Tashima, MD, Brown Medical School, Providence, Rhode Island; Pablo Tebas, MD, University of Pennsylvania, Philadelphia, Pennsylvania; Lucia V. Torian, PhD, New York City Department of Health, New York, New York.

CDC Staff Members: Theresa Diaz, MD; M. Kathleen Glynn, DVM; Lisa M. Lee, PhD; Matthew T. McKenna, MD; Andrew Mitsch, MPH; Eileen Schneider, MD; Patrick Sullivan, DVM, PhD.

CDC Adult/Adolescent HIV Surveillance Case Definition Consultation, June 2006

External Consultants: A. Cornelius Baker, National Black Gay Men's Advocacy Coalition, Washington, DC; John Barnhart, MPH, National Alliance of State and Territorial AIDS Directors, Washington, DC; Spencer Bennett, MPH, Florida Bureau of Laboratories, Jacksonville, Florida; Laura Cheever, MD, ScM, Health Resources and Services Adminstration, Rockville, Maryland; Michael D'Arata, FNP, Family Care Network, Oakland, California; Isabelle Devaux, PhD, EuroHIV, Saint Maurice Cedex, France ; Damon Dozier, National Minority AIDS Council, Washington, DC; Judith Feinberg, MD, University of Cincinnati College of Medicine, Cincinnati, Ohio; Eberhard Fiebig, MD, University of California, San Francisco General Hospital, San Francisco, California; Lance Gable, JD, Georgetown University Law Center, Washington, DC; James Gibson, MD, South Carolina Department of Health and Environmental Control, Columbia, South Carolina; Charles Gilks, D Phil, World Health Organization, Geneva, Switzerland; David Harvey, AIDS Alliance for Women, Children Youth and Families, Washington, DC; Jennifer Kates, MPA, MA, Kaiser Family Foundation, Washington, DC; Lynda Kettinger, MPH, South Carolina Department of Health and Environmental Control, Columbia, South Carolina; Peter Leone, MD, University of North Carolina, Chapel Hill, North Carolina; Eve Mokotoff, MPH, Michigan Department of Community Health, Detroit, Michigan; Israel Nieves-Rivera, San Francisco Department of Public Health, San Francisco, California; Jennifer Pennock, MSc, Public Health Agency of Canada, Ottawa, Ontario, Canada; Monica S. Ruiz, PhD, The Foundation for AIDS Research, Washington, DC; R. Luke Shouse, MD, Georgia Division of Public Health, Atlanta, Georgia; Gregory I. Smiley, MPH, American Academy of HIV Medicine, Washington DC; Andrew Spieldenner, MA, National Association of People With AIDS, Silver Spring, Maryland; Edward Tepporn, Asian & Pacific Islander American Health Forum, San Francisco, California; Steven Tierney, EdD, San Francisco AIDS Foundation, San Francisco, California.

CDC Staff Members: Bernard Branson, MD; Theresa Diaz, MD; M. Kathleen Glynn, DVM; Duncan MacKellar, MPH; Stephen McDougal, MD; Matthew T. McKenna, MD; Andrew Mitsch, MPH; Allyn Nakashima, MD; Michelle Owen, PhD; Travis Sanchez, DVM; Eileen Schneider, MD.

CDC Pediatric HIV Surveillance Case Definition Consultation, April 2005

External Consultants: John Barnhart, MPH, National Alliance of State and Territorial AIDS Directors, Washington, DC; Mark Cotton MB ChB, Stellenbosch University, Tygerberg, South Africa; Siobhan Crowley, MB, MRCP, World Health Organization, Geneva, Switzerland; Brian Feit, MPA, Health Resources Services Administration, Rockville, Maryland; Susan Fiscus, PhD, University of North Carolina at Chapel Hill School of Medicine, Chapel Hill, North Carolina; Pat Flynn, MD, St. Jude Children's Research Hospital, Memphis, Tennessee; Toni Frederick, PhD, University of Southern California, Los Angeles, California; Edward Handelsman, MD, SUNY Downstate/Kings County Hospital Center, Brooklyn, New York; Celine Hanson, MD, Texas Children's Hospital, Houston, Texas; Peter Havens, MD, Medical College of Wisconsin; Children's Hospital of Wisconsin, Milwaukee, Wisconsin; Israel Kalyesubula, MB ChB, Makerere University, Kampala, Uganda; Sharon Melville, MD, Texas Department of State Health Services, Austin, Texas; Lynne Mofenson, MD, National Institutes of Health, Rockville, Maryland; Steven Nesheim, MD, Emory University School of Medicine, Atlanta, Georgia; Marie-Louise Newell, PhD, Institute of Child Health, London, United Kingdom; James Oleske, MD, MPH, New Jersey Medical School, Newark, New Jersey; Mary Paul, MD, Texas Children's Hospital, Houston, Texas; Vicki Peters, MD, New York City Department of Health and Mental Hygiene, New York, New York; Kenneth Rich, MD, University of Illinois at Chicago, Chicago; Illinois, Damaris Richardson, Department of Health and Mental Hygiene, Baltimore, Maryland; Zoe Rodriguez, MD, University of Puerto Rico, San Juan, Puerto Rico; Christine Rouzioux, PhD, Hôpital Necker–Laboratorie de Virologie, Paris, France; Andrea Ruff, MD, Johns Hopkins University Bloomberg School of Public Health, Baltimore, Maryland; Gwendolyn. Scott, MD, University of Miami School of Medicine, Miami, Florida; Mary Elizabeth Smith, MD, National Institutes of Health, Bethesda, Maryland; Russell Van Dyke, MD, Tulane University Health Sciences Center, New Orleans, Louisiana; Barbara Warren, New York State Department of Health, Albany, New York; Patricia Whitley-Williams, MD, New Brunswick, New Jersey.

CDC Staff Members: Bernard Branson, MD; Michael Campsmith, DDS; Kenneth Dominguez, MD; Mary Jo Earp, MPH; Lorena Espinoza, DDS; Mary Glenn Fowler, MD; M. Kathleen Glynn, DVM; Norma Harris, PhD; Matthew T. McKenna, MD; Andrew Mitsch, MPH; Alpa Patel-Larson, MPH; Ruby Phelps; Nan Ruffo; Stephanie Sansom, PhD; Suzanne Whitmore, DrPH.

Members of the CDC Pediatric Surveillance Case Definition for HIV Infection and AIDS Working Group

Michael Campsmith, DDS; Kenneth Dominguez, MD; Steve McDougal, MD; Andrew Mitsch, MPH; Alpa Patel-Larson, MPH; Nan Ruffo; Alexis Reedy Benavides, MPH; Allan Taylor, MD; Suzanne Whitmore, DrPH.

The *Morbidity and Mortality Weekly Report (MMWR)* Series is prepared by the Centers for Disease Control and Prevention (CDC) and is available free of charge in electronic format. To receive an electronic copy each week, send an e-mail message to *listserv@listserv.cdc.gov*. The body content should read *SUBscribe mmwr-toc*. Electronic copy also is available from CDC's Internet server at *http://www.cdc.gov/mmwr* or from CDC's file transfer protocol server at *ftp://ftp.cdc.gov/pub/publications/mmwr.* Paper copy subscriptions are available through the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402; telephone 202-512-1800.

Data in the weekly *MMWR* are provisional, based on weekly reports to CDC by state health departments. The reporting week concludes at close of business on Friday; compiled data on a national basis are officially released to the public on the following Friday. Data are compiled in the National Center for Public Health Informatics, Division of Integrated Surveillance Systems and Services. Address all inquiries about the *MMWR* Series, including material to be considered for publication, to Editor, *MMWR* Series, Mailstop E-90, CDC, 1600 Clifton Rd., N.E., Atlanta, GA 30333 or to *mmwrq@cdc.gov.*

All material in the *MMWR* Series is in the public domain and may be used and reprinted without permission; citation as to source, however, is appreciated.

Use of trade names and commercial sources is for identification only and does not imply endorsement by the U.S. Department of Health and Human Services.

References to non-CDC sites on the Internet are provided as a service to *MMWR* readers and do not constitute or imply endorsement of these organizations or their programs by CDC or the U.S. Department of Health and Human Services. CDC is not responsible for the content of these sites. URL addresses listed in *MMWR* were current as of the date of publication.

☆U.S. Government Printing Office: 2009-523-019/41141 Region IV ISSN: 1057-5987

Chapter 6 Additional Contractual Requirements

In addition to investigating and reporting HIV/AIDS cases, surveillance sites are contractually required to perform additional surveillance related activities. These activities include:

- Provider Education
- Active Surveillance
- Monthly/Quarterly Reporting

HIV/AIDS Surveillance sites are reviewed annually to evaluate compliance with all contractual requirements.

6-1 Provider Education

HIV/AIDS surveillance sites are required to visit major reporting sources at least annually to inform them of the reporting requirements, provide reporting materials, and reinforce the need to report STDs, including HIV/AIDS. Surveillance sites should hold supplemental training sessions if issues, such as security breaches, arise. Reporting materials must be distributed to local health clinics, public and private hospitals, private physicians, laboratories and other reporting sources in the local surveillance areas. In addition, surveillance sites should identify new providers/facilities and provide them with all necessary information regarding reporting.

6-2 Active Surveillance

In addition to education, HIV/AIDS Surveillance sites must maintain regular contact with major reporting facilities to inquire about any new cases. Surveillance staff should inquire at HIV/AIDS treatment facilities at least monthly to identify any unreported cases. Surveillance sites must strive to identify all reporting facilities within their region to ensure that appropriate surveillance and case follow-up is occurring.

6-3 Monthly and Quarterly Reporting

A. Monthly Reporting Database

The purpose of the monthly reporting database is to track monthly activities, evaluate workloads, develop an overall picture of daily activities at the local and regional offices and provide updates on specific contractual measures. Monthly, this information is reviewed by Central Office staff and the DSHS contract management unit. Facility contacts, provider education and active surveillance information is used when completing the pre-site portion of the Site Review Tool. In addition, sites are contractually responsible for timely submission of Monthly Staff Activities Reports that can be generated within the Monthly Reporting Database. Timely submission of reports is evaluated during the site review.

Program mangers may also find that reports on staff activities are helpful when evaluating workloads, identifying needs of the HIV surveillance program and deciding responsibilities for HIV surveillance staff. Each quarter, program managers are responsible for signing and submitting quarterly reports that are generated in the Monthly Reporting Database.

A separate database should be used for each position within HIV Surveillance. Monthly Staff Activities Reports are due to Central Office by the **10th** of each month. If the Monthly Staff Activities Report has not been sent by the 12th of the month, it will be

considered late. *Appendix A: Monthly Reporting Database Instructions* will provide additional information on using the Monthly Reporting Database.

B. Monthly Quality Assurance and Completeness Reports

Monthly, Central Office generates several different reports that must be reviewed by surveillance staff and program managers. The following reports packages are sent to the sites:

- Program Summary Monthly Report Package: These reports are sent via email to program managers and surveillance staff by the first Wednesday of the month. These reports allow program managers and surveillance staff to evaluate how effectively the surveillance program is operating. Two reports are contained within this package:
  - Outcome Measures Summary that shows how all surveillance programs are progressing toward meeting quality assurance and completeness standards that are evaluated during site reviews. Each measure on the Outcome Measures Summary report can compared to the standard (noted in the report titles) and other like programs in the state; and
  - Surveillance Report Summary of the number of cases reported within given time frames, compared to previous months. This information should be used to ensure that the surveillance process is operating appropriately.
- Quality Assurance Monthly Report Package: These reports are provided via the TxPHIN to HIV surveillance staff by the 17th of each month. These reports identify specific cases that have missing/incorrect information. All cases should be corrected as soon as possible to ensure compliance with quality assurance measures in the site review tool. The following reports are included:
  - Perinatal Quality Assurance: Summary reports are generated from eHARS and contain Pediatric Case Report forms with errors and Pediatric Case Report Forms regarding children with indeterminate HIV status.
    - The summary report of Pediatric Case Report Forms with errors should be reviewed, corrections should be made, and if necessary re-abstraction of records should take place, all activities occurring within 1 month of receipt.
  - Outcome Measures Summary Details: This report provides a detailed list of cases that are missing key variables, such as risk, race, vital status, sex, and residence at diagnosis.
  - EHARS QA and Pedi EHARS QA Report: This report details the documents or cases that require correction in eHARS due to a data entry error. Note that only sites who enter data locally into eHARS will receive this report.
- Testing and Treatment History (TTH) information: All TTH data elements reported on the ACRF should be reviewed for accuracy and completeness. Each month, as part of the Program Summary Monthly Report package, surveillance sites will receive a report on their progress towards meeting TTH quality assurance completeness standards that are evaluated during site reviews.

C. Quarterly Reports

Quarterly, Central Office will send the following reports to sites for follow up.

- Quarterly Program Managers Report: This report is sent quarterly via email to all program managers. This report details how the site is progressing toward meeting the measures in the site review tool and objectives established by the Texas HIV Surveillance Program. Program managers must review and sign the report. A scanned copy must be emailed to the below individuals by the third Wednesday of the month in which the report was received:
  - HIV Surveillance Data Reporting Manager: Miranda.Fanning@dshs.state.tx.us
  - Contract Monitoring Unit: Linda.Horton@dshs.state.tx.us
- Quarterly Activities Report: This report is generated in the Monthly Reporting database. It details surveillance staff activities during the quarter. Program managers must review and sign a copy of the report for each surveillance staff member. The signed copy should be emailed with the Quarterly Program Managers Report to:
  - HIV Surveillance Data Reporting Manager: Miranda.Fanning@dshs.state.tx.us
  - Contract Monitoring Unit: Linda.Horton@dshs.state.tx.us
- Missing Testing and Treatment History (TTH) data elements: Surveillance sites are required to complete the TTH data elements for all newly-reported adult HIV cases. Quarterly, DSHS staff will identify newly reported HIV cases that are missing TTH data elements and provide surveillance sites with a list of these cases. The list will contain the patient name, DOB, Stateno, and facility of diagnosis from eHARS. The surveillance site will need to complete an update ACRF with the TTH data elements for these cases within 30 days.

6-4 Site Reviews

Central Office staff visit each HIV/AIDS surveillance site every other year to conduct an evaluation of compliance with contractual agreements. Evaluations are comprised of seven components:

1) Security
2) Reporting
3) Other Contractual Obligations
4) Data quality
5) Program Documentation
6) Management
7) Surveillance

The guidelines and standards for each item were developed based on the HIV/STD Epidemiology and Surveillance Branch's HIV and STD Program Operating Procedures and Standards, the CDC's Technical Guidance for HIV/AIDS Surveillance Programs, and the HIV/AIDS Program's Perinatal Surveillance, Incidence, and Core surveillance grant objectives.

Each item is evaluated on the following rating scale:

- E=Exceeds Standards
- M=Meets Standards

- NM=Does Not Meet Standards
- NA=Not Applicable
- NE=Not Evaluated

The evaluation tool used for the annual review can be found in Appendix B: *Program Review Tool*. To conduct the site review, Central Office staff complete the evaluation tool from reporting statistics generated at Central Office and on-site discussion of current procedures and operating protocol. If the HIV/AIDS surveillance site receives a rating of "Partially Meets Standards" or "Does Not Meet Standards", Central Office staff will collaborate with the HIV/AIDS surveillance site's staff to develop an action plan that will ensure contractual compliance. Following the review, Central Office staff will provide the HIV/AIDS surveillance site with a summary of findings and action items. A copy of the current review schedule can be found in Appendix C.

Appendix A- Using the Monthly Reporting Database

The monthly reporting database has two reporting components: a facility contacts tracker and a monthly activities tracker. In addition, monthly reports are generated from the database.

Entering Facility Contacts

The facility contacts section should be used to document contacts you made to facilities for purposes other than medical record abstractions and requesting preliminary data identified cases. In this section, you can record contacts for Education, Training and Active Surveillance.

1) Select the box next to *Enter Facility Contacts*.
2) In the form titled "Facility Contacts- for Education, Training and Active Surveillance, select the facility name. If the facility name does not appear in the drop down menu, type in the name.
3) Enter the date of contact if different from today.
4) Select the Contact Type from the drop down menu.
5) Select the Purpose of the contact from the drop down menu.
    a. If *Request Linelist to identify unreported cases (Active Surveillance)* is selected, enter number of new cases identified.
    b. If *Provide reporting requirements to new facility/new staff* or *Educating/training updates for facilities/staff* is selected, enter the number of staff trained.
    c. If other is selected, include the purpose of the contact in the *Description* box.
6) Enter any notes about the contact in the description box.

Entering Activities

The Monthly Activities section should be used to document how you spent your time throughout the month. To ensure that all monthly activities are captured and reported as accurately as possible, the database should be updated at least weekly. However, daily updates are recommended.

1) Select the box next to *Enter Activities*.
2) In the form titles "Daily Activities Log", select the type of activity from the drop down menu.
3) Enter the date the activity was done, if different from today.
4) Enter the number of hours spent on the activity.
5) Enter additional notes. If *Other* is selected from the *Type of Activity* drop down menu, you must enter the activity in the *Additional Notes* field.

Running Monthly Reports

Monthly Reports should be run at the sites and sent to central office by the 10th of each month.

1) Select the month for which the report should be run.
2) Select the year for which the report should be run.
3) Select the *Run* button.
4) Review the report. If everything looks correct, print and scan the report and email it to the following individuals:
    a. HIV Surveillance Data reporting manager- Miranda.fanning@dshs.state.tx.us
    b. Contracts Monitoring Unit- Linda.Horton@dshs.state.tx.us

Running Quarterly Reports

Quarterly Reports should be run at the sites and sent to central office by the third Wednesday following the end of the quarter.

5) Select the quarter for which the report should be run.
6) Select the year for which the report should be run.
7) Select the *Run* button.
8) Review the report. If everything looks correct, print the report. Program managers should review the report and provide a signed copy to the following individuals:
    a. HIV Surveillance Data reporting manager- Miranda.fanning@dshs.state.tx.us
    b. Contracts Monitoring Unit- Linda.Horton@dshs.state.tx.us

Chapter 7

Chapter 7 Security Policies and Procedures

The HIV/STD Epidemiology and Surveillance Branch has developed policies and procedures to protect the security and confidentiality of HIV/STD data. All surveillance sites are required to either adopt these security policies and procedures or develop their own procedures that are in compliance with federal and state HIV/AIDS confidentiality guidelines and approved by Central Office. The following policies and procedures developed by Central Office describe how to ensure physical security, to maintain the security and confidentiality of HIV/STD data, circumstances under which HIV/STD data can be released, and procedures for addressing potential security breaches:

- HIV/STD Confidential Information Security Policy
    - HIV/STD Epidemiology and Surveillance Confidential Information Security Procedures
    - HIV/STD Public Health Follow-Up (PHFU) Confidential Information Security Procedures
- Overall Responsible Party for HIV/AIDS Surveillance Data
- Release of HIV/AIDS and STD Data
- HIV/STD Breach of Confidentiality Response Policy

See *Appendix A Security Policies and Procedures*, for the above policies and procedures.

Maintaining the security and confidentiality of HIV/STD data should be a priority for all surveillance staff and every effort should be made to adhere to the security policies and procedures.

Appendix A:
Security Policies and Procedures

TEXAS Department of State Health Services	*Policy Number*	303.001
	Effective Date	February 10, 1999
	Revision Date	July 2, 2008
	Subject Matter Expert	Surveillance Specialist
	Approval Authority	Branch Manager
HIV/STD Breach of Confidentiality Response Policy	*Signed by* Sharon K. Melville, MD, MPH	

1.0 Purpose

This policy describes the actions required of the Texas Department of State Health Services (DSHS) HIV/STD Program and entities with whom DSHS has a contractual or professional relationship to handle confidential HIV/STD surveillance, epidemiological, medication, and public health follow-up data in the event of a suspected breach. This policy also outlines how to address negligent or purposeful release of confidential client information.

This policy has been written to align with requirements in the Department of State Health Services (DSHS) *HIV and STD Program Operating Procedures and Standards (POPS)* (http://www.dshs.state.tx.us/hivstd/pops/default.shtm), the DSHS IR-2204 Information Security Policy (http://online.dshs.state.tx.us/it/standards/securitystd.htm), the Centers for Disease Control and Prevention's (CDC) Program Operations Guidelines for STD Prevention (http://www.cdc.gov/std/Program/overview/TOC-PGoverview.htm), and the CDC's *Technical Guidance for HIV/AIDS Surveillance Programs* (Atlanta, GA; 2006), wherever possible and/or appropriate.

2.0 Background

In fulfilling its mission to prevent, treat, and control the spread of HIV, STDs and other communicable diseases, the DSHS HIV/STD program, its contractors and external partners obtain confidential information regarding individuals they serve. These individuals trust that the HIV/STD program will take every precaution to protect that information in order to retain their confidentiality. The HIV/STD program must be vigilant in maintaining the integrity of systems that contain this confidential information.

3.0 Authority

Vernon's Texas Statutes and Codes Annotated (V.T.C.A.), Penal Code, Chapter 16, Chapter 33; V.T.C.A. Health and Safety Code, 81.046 and 81.103-81.104; V.T.C.A., Texas Government Code, Chapter 552

4.0 Definitions

Breach of Confidentiality- A breach of protocol that results in the improper disclosure of confidential information. The result is confidential information being: 1) accidentally or purposefully released verbally, electronically, or by paper medium, to an entity or person that by law does not have a right or need to know, or 2) purposefully accessed either in person or electronically by an entity or person that by law does not have a right or need to know.

Breach of Protocol - A departure from the established policies and procedures that may result in the improper disclosure of confidential information; an infraction or violation of a standard or obligation. This includes any unauthorized use of data, including de-identified data.

Central Office- The HIV/STD Program, Department of State Health Services (DSHS) main office located in Austin Texas.

Confidential Information- Any information which pertains to a patient that is intended to be kept in confidence or kept secret and could result in the identification of the patient should that information be released. and.

Confidentiality- The ethical principle or legal right that a physician or other health professional or researcher will prevent unauthorized disclosure of any confidential information relating to patients and research participants..

External- Entities outside of the DSHS Central Office that the HIV/STD program contracts with or works in association with to conduct public health activities related to HIV/STD surveillance, epidemiology, public health follow-up and the medication program.

Internal- Refers to staff and occurrences located at DSHS Central Office in Austin, Texas.

Local Responsible Party (LRP)**-** An official who accepts responsibility for implementing and enforcing HIV/STD security and confidentiality polices and procedures related to HIV/STD surveillance, epidemiology, public health follow-up and medication program data and information and has the responsibility of reporting and assisting in the investigative breach process.

Negligence- The failure to use reasonable care. The failure to do (or not to do) something that a reasonably prudent person would do (or not do) under like circumstances. A departure from what an ordinary reasonable member of the community would do in the same community. Negligence is a 'legal cause' of damage if it directly, and in natural and continuous sequence, produces or contributes substantially to loss, injury, or damage, so it can reasonably be said that if not for the negligence, the loss, injury, or damage would not have occurred.

Purposeful-Deliberate and with the intention to cause harm to another.

Security Officer- Internally, the individual designated by each group in the HIV/STD program to be part of the Security Team. The Security Officer assists in the investigative process of reported suspected breaches when the incident is directly related to the security officer's program (group) area.

Security Team- Internally, the Security Team consists of a security officer, group manger, and the Local Responsible Party. Externally, this team consists of appropriate staff designated to serve in this team. The Security Team is responsible for investigating suspected breaches, gathering all facts related to the incident, drawing conclusions, making recommendations for further action, and providing a closing report.

Suspected Breach: An alleged infraction or violation of a standard that may result in unauthorized disclosure of confidential information

5.0 Policy

The DSHS HIV/STD program ensures that appropriate DSHS staff members will respond to suspected breaches by reporting, investigating and providing follow-up to these incidents. This policy prescribes guidelines for addressing deviations from the established policies and procedures as specified in the DSHS HIV/STD Confidential Information Security Policy and the Release of HIV/AIDS and STD Data Policy.

6.0 Persons Affected/Applicability

This policy applies to all DSHS employees, IT staff, temporary employees, volunteers, students, DSHS program contractors, and any other persons who could potentially view and/or have access to HIV/STD confidential information.

7.0 Responsibilities

All persons affected by this policy, as specified in section 6.0, are responsible for the reporting of suspected breaches.

Internal and external sites are responsible for designating a Local Responsible Party (LRP). Internally the HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch Managers will be designated as the LRPs. The HIV/STD Epidemiology and Surveillance Branch Manager will be responsible for investigating and responding to breaches related to HIV/STD surveillance and epidemiological data and information. The HIV/STD Comprehensive Services Branch Manager will be responsible for investigating and responding to breaches related to medication data and information. The HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch managers will be jointly responsible for investigating and responding to breaches related to public health follow-up information and data. The LRP will be responsible for implementing and enforcing security and confidentiality polices and procedures and for investigating suspected breaches.

Internal and external sites are responsible for designating a Security Team. The Security Team will be responsible for assisting the LRP investigate suspected breaches, gather all facts related to the incident, draw conclusions, make recommendations for further action, and provide a closing report.

8.0 Reporting and Investigating a Suspected Breach

Internally, the DSHS HIV/STD Program will create and identify a Security Team, procedure, and documents for tracking, reporting, and investigating suspected breaches. Internally, the Security Team consists of a security officer, group manger, and the LRP. The group manager and the Security Officer will assist in the investigative process of reported suspected breaches when the incident is directly related to their respective program (group) area. When reporting a suspected breach, confidential patient information will not be submitted on the DSHS HIV/STD Program breach reporting form. In response to a suspected breach, the DSHS HIV/STD Program will follow internal procedures for reporting, documenting and investigating the incident. If a suspected breach has not been identified but confidential information is potentially at risk of being divulged, the LRP will be notified directly. The breach report form will not be used in these instances.

Externally, policies and procedures that are consonant with the DSHS HIV/STD Program policy for documenting, investigating, and reporting suspected breaches will be created. External sites will designate an LRP and a Security Team responsible for reporting and investigating a suspected breach. Externally, the Security Team consists of appropriate staff designated to serve in this team. The external LRP will inform the appropriate internal LRP of a suspected breach within 24 hours after the incident is first reported.

8.1 Action Steps in Response to a Suspected Breach

Internally, the DSHS HIV/STD Program will follow established procedures for responding to a suspected breach. The Security Team will be responsible for determining the validity of a suspected breach and determining the type of breach that has occurred. Recommended corrective actions will be taken based on the type of breach determined to have occurred.

Externally, regional and contracting offices will implement policies and procedures that adhere to the guidelines set forth in the DSHS HIV/STD Program policy for responding to suspected breaches. The external LRP will communicate the Security Team's recommended corrective actions to the appropriate internal LRP. Recommended corrective actions will be based on local personnel policies for dealing with employees who violate protocols and/or confidentiality. Once the external and internal LRPs are in agreement with the proposed recommendations, the external LRP will be responsible for providing a final closing report to the internal LRP. However, when a response to a confirmed breach is deemed insufficient by the internal LRPs, DSHS may place the DSHS contracted site on sanctions as referenced in Policy AA-5116 (Sanctions and Remedies for Contract Non-Compliance) http://online.dshs.state.tx.us/policy/agency/aa-5116.htm

8.2 Follow-up to a Breach and Maintenance of Files

Internally, the DSHS HIV/STD Program will follow established procedures requiring follow-up to a confirmed breach. In the event of a confirmed breach, the Group Manager is responsible for providing monthly follow-up reports to the LRP documenting progress on the corrective action plan. Monthly follow-up reports will be submitted until corrective actions are concluded or deemed sufficient by the internal LRP. Subsequently, all hard copies of final reports and electronic data will be maintained by the HIV/STD Epidemiology and Surveillance Branch Overall Responsible Party (ORP) and/or designee(s) as outlined in the DSHS HIV/STD Program policies and procedures.

External sites will adopt policy and procedures requiring follow-up to a confirmed breach that meet the guidelines of the DSHS HIV/STD Program policy and procedures. The external LRP will be responsible for providing monthly follow-up reports to the appropriate internal LRP until corrective actions are concluded or deemed sufficient by the internal LRP. The DSHS HIV/STD Program will maintain breach-reporting forms of suspected breaches in the DSHS contractor file. Breach reporting forms that are kept with the DSHS contractor file will be redacted of any confidential information pertaining to the person who committed the suspected breach.

To prevent further breaches in protocol, internal and external sites involved in handling confidential information will be thoroughly retrained on the policies of the agency and the program. As part of the training, examples should be given to illustrate what constitutes a breach and describe the consequences if someone releases confidential information. It should be stressed that the individual and the agency may be held liable for breaches.

9.0 Procedures-Internal

Reporting a Suspected Breach

1.	The DSHS staff member who receives the initial notice of the suspected breach will document the incident using the Breach Report Form ("Section 1: Initial Report").
2.	The initial part of the breach report must be completed and submitted via e-mail to the appropriate Group Manager, within 24 hours of the incident. If the Group Manager is not available, then the acting Group Manager is notified via e-mail within 24 hours of the incident.
3.	The DSHS staff person must receive an e-mail confirmation from the Group Manager indicating receipt and review of the initial Breach Report Form. If no confirmation is received within 24 hours, the initial Breach Report Form must be sent directly to the LRP.
4.	The Group Manager will review the initial Breach Report and make a recommendation to the LRP for closing out the report when sufficient and reasonable information confirms that a breach has not occurred.
5.	The Group Manager will notify the appropriate LRP(s) and any field staff as appropriate. The Group Manager will also provide the appropriate LRP(s) with the initial breach report via e-

	mail and insure that the other internal LRP is also cc'ed and receives notice of the suspected breach. (The Group Manager must notify and provide the initial breach report to the LRPs within 24 hours after receiving the completed initial Breach Report Form from the DSHS staff member.)
6.	If the appropriate LRP for that Group is not available, the Group Manager will need to send a separate e-mail to the other internal LRP indicating that the appropriate LRP is not available and response will be needed on his/her part.
7.	If the internal LRPs are not available, the Group Manager will notify the Unit Manager or the next level of management available through telephone and e-mail.
8.	The staff member initially submitting the request must receive an e-mail confirmation from the LRP indicating receipt and review of the initial Breach Report Form.

Investigating a Suspected Breach

1.	After the LRP has received the breach report, the LRP will inform the Security Team of the suspected breach.
2.	The Security Team will be responsible for further investigating the incident. (The Security Team may request further information regarding the incident to be submitted.)
3.	The Security Team will review the initial breach report and complete "Section 2: Security Team Closing Report". The investigation should be finished no later than 7 days following the initial incident date.
4.	The final completed report (Sections 1 and 2) will be sent to both internal LRPs via e-mail.
5.	All media calls related to an internal suspected breach must be referred to the CSHS Communications Public Relations Officer according to DSHS Policy AA-5036 (News Media Policy) http://online.dshs.state.tx.us/policy/agency/aa-5036.htm
6.	Any breach of confidentiality will be investigated immediately to assess causes and implement corrective actions. If a breach of confidentiality is related to a federally sponsored program, the LRP will report it promptly to the appropriate federal program contact.

Action Steps Specific to the Type of Breach

1.	Suspected Breach (Non-breach in protocol): a. A suspected breach is reported and the Security Team investigates the suspected breach. b. The Security Team determines that the suspected breach is neither a breach of protocol nor a breach of confidentiality. c. The Security Team will ensure that the Group Manager communicates the findings to the appropriate DSHS staff member. d. The LRP will be responsible for closing out the report.
2.	Breach in Protocol: a. A suspected breach is reported and the Security Team investigates the suspected breach. b. The Security Team determines that the suspected breach is a breach in protocol but not a breach in confidentiality. (In this case the Security Team has determined that no confidential information has been divulged in any manner but a breach in protocol poses a risk to a breach in confidentiality and recommendations will need to be made accordingly.) c. When only a breach in protocol has occurred, the Security Team will need to determine if the breach was negligent or purposeful. d. The Security Team will recommend the necessary actions to be taken based on the type of breach (negligent or purposeful) to the Group Manager. e. Subsequently, it is the responsibility of the Group Manager to monitor the employee and assure that further breaches in protocol do not occur that may ultimately result in a breach of confidentiality. f. The Group Manager will also assure that the employee causing this breach in

	protocol receives emergency training on security and confidentiality. g. Additionally, disciplinary action may need to be taken by the Group Manager especially when repeated breaches in protocol have occurred. If the employee continues to pose a threat to security of confidentiality, the employee's access to HIV/STD Program information will be limited or rescinded until further personnel actions have been determined.
3.	Breach in protocol and confidentiality: a. A suspected breach is reported and the Security Team investigates the suspected breach. b. The Security Team determines that the suspected breach is a breach in protocol and a breach in confidentiality. (In this case the Security Team has determined that confidential information has been divulged and an immediate response is necessary.) c. When the suspected breach is found to be both a breach of protocol and breach of confidentiality, the Security Team will make appropriate recommendations regarding actions that will need to be taken based on whether the breach is determined to be purposeful or due to negligence. d. Regardless of the type of breach (purposeful or negligent), the following recommendations may be required based on the severity of the breach of confidentiality: • The employee's access to physical and electronic resources must be limited or rescinded until an investigation of the incident is complete. Options for handling the situation include: immediately reassigning the employee to a temporary duty station; obtaining permission from the Unit Chief (to whom the employee is assigned) to send the employee home pending investigation of the breach; or calling law enforcement in extreme situations. • At the discretion of the LRP the following entities may be notified: the Communications Office, the Office of General Counsel, the Commissioner of Health, the Associate Commissioner for Disease Control and Prevention, the Director, Prevention and Intervention Section, the Health Promotion Unit Manager and the HIV/STD Epidemiology and Surveillance Unit Manager and other appropriate senior departmental staff, if appropriate. • Implement new or additional processes to address any deficiencies in the HIV/STD program security and confidentiality policies and procedures.

Follow-Up to a Breach and Maintenance of Files

1.	If a breach has occurred, the Group Manager will submit a follow-up report via e-mail to both LRPs on a monthly basis. The follow-up report will detail the corrective steps (Section 3 of Breach Report Form) that have been taken to resolve the problem to prevent the breach from occurring again.
2.	On a monthly basis, the internal LRPs will confirm receipt of the follow-up Breach Report Form and indicate if the response is appropriate. Monthly follow-up reports will be submitted until corrective actions are concluded or deemed sufficient by the internal LRP(s).
3.	The ORP or designee will retain a file of all completed breach response forms in a locking file cabinet. (Breach Report Forms will be maintained separate from the employees personnel file.)
4.	The ORP's designee will enter all information into the Breach Report Database. The Breach Report Database will be password protected and only the ORP, LRP(s) and designee(s) will have access to the database.
5.	The Group Manager will be responsible for periodically running reports based on the Breach Report Database and determine if any patterns in breaches exist that need to be further addressed.

10.0 Revision History

Date	action
07/02/08	Revisions too numerous to list; therefore treated as new policy. Policy previously identified as 020.051

TEXAS Department of State Health Services	*Policy Number*	302.001
	Effective Date	April 9, 1999
	Revision Date	July 2, 2008
Release of HIV/AIDS and STD Data	*Subject Matter Expert*	Surveillance Specialist
	Approval Authority	Branch Manager
	Signed by	Sharon K. Melville, MD, MPH

1.0 Purpose

This policy describes guidelines for the release or publication of data associated with HIV/AIDS and STD surveillance, epidemiologic, public health follow-up, and the Texas HIV Medication Program (THMP). This policy aligns with requirements in the DSHS HIV and STD Program Operating Procedures and Standards (POPS) (http://www.dshs.state.tx.us/hivstd/pops/default.shtm), the Centers for Disease Control and Prevention's (CDC) Program Operations Guidelines for STD Prevention, (http://www.cdc.gov/std/Program/overview/TOC-PGoverview.htm), and the CDC's Technical Guidance for HIV/AIDS Surveillance Programs (Atlanta, GA; 2006) wherever possible and/or appropriate.

2.0 Authority

All information obtained and compiled by DSHS related to a disease report is confidential and may be used or released only as permitted by Health and Safety Code §81.046. Additionally, DSHS is legally bound by federal assurances of confidentiality (Sections 306 and 308(d) of the Public Health Service Act, 42 US Code 242k and 242m(d)) which prohibit disclosure of any information that could be used to directly or indirectly identify patients. This policy has been written in accordance with the Health and Safety Codes §81.046 and §81.103 and the Texas Administrative Codes §97.146 and §98.13 of Title 25.

3.0 Definitions

Aggregate Data - data which are based on combining individual level information; Aggregate data may contain potentially identifying information, particularly if the aggregated data are very detailed or for a small subset of individuals.

Central Office – the HIV/STD Program, Department of State Health Services (DSHS) main office located in Austin, Texas.

Confidential Information – any information which pertains to a patient that is intended to be kept in confidence or kept secret and could result in the identification of the patient should that information be released.

Confidentiality - the ethical principle or legal right that a physician or other health professional or researcher will prevent unauthorized disclosure of any confidential information relating to patients and research participants

De-identified (Pseudo-anonymous) Data - individual record-level data which has been stripped of personal identifiers (e.g., name, address, social security number) but may contain potentially identifying information (e.g., age, sex, race/ethnicity, locality information) that when combined with other information may identify an individual. If the combining of information could identify an individual, these data are considered confidential.

Demographics – refers to selected population characteristics, including race/ethnicity, sex, and age.

External – entities outside of the DSHS Central Office that the HIV/STD Program contracts with or works in association with to conduct public health activities related to HIV/STD surveillance, epidemiology, public health follow-up and the medication program.

Fifty Rule – refers to the acceptable threshold for the release of aggregate HIV/AIDS and STD surveillance, epidemiologic, and public health follow-up data. The underlying population of the statistic released must be a population of greater than fifty people. The underlying population must also be at least twice the number of cases.

Geocode - is a representation format of a geospatial coordinate measurement used to provide a standard representation of an exact geospatial point location at, below, or above the surface of the earth at a specified moment of time.

Geographic Information System (GIS) – is an information system capable of integrating, storing, editing, analyzing, sharing, and displaying geographically-referenced data.

HIV/STD Program – consists of the two branches of the DSHS Prevention and Preparedness Unit: the HIV/STD Comprehensive Services Branch and the HIV/STD Epidemiology and Surveillance Branch.

Institutional Review Board (IRB) - is a group that has been formally designated to approve, monitor, and review biomedical and behavioral research involving humans with the aim to protect the rights and welfare of the subjects.

Local Responsible Party (LRP) – an official who accepts responsibility for implementing and enforcing HIV/STD policies and procedures related to the security and confidentiality of HIV/STD surveillance, epidemiology, public health follow-up and medication program data and information and has the responsibility of reporting and assisting in the investigative breach process.

Personal Identifier - a datum or collection of data which allows the possessor to determine the identity of a single individual with a specified degree of certainty; a personal identifier may permit the identification of an individual within a given database. Bits of data, when taken together, may be used to identify an individual. Personal identifiers may include name, address or place of residence, social security number, telephone number, fax number, and exact date of birth.

Population - a group of people defined by demographic characteristics such as age, race, sex, or location of residence

Potentially Identifying Information – information which, when combined with other information, could potentially identify an individual or individuals. This includes but is not limited to such information as medical record/case numbers and demographic or locality information that describe a small subset of individuals (e.g., block data, zip codes, race/ethnicity data).

Surveillance - the ongoing and systematic collection, analysis, and interpretation of health data in the process of describing and monitoring a health event. This information is used for assessing public health status, triggering public health action, defining public health priorities and evaluating programs.

4.0 Policy

The policy of DSHS is to ensure that HIV/AIDS and STD data are released and/or published while maintaining patient confidentiality. The policy is also to ensure that individual record-level data containing personal identifiers are only released with proper legal authority. HIV/STD Program staff must assess the potential impact of proposed data releases on confidentiality, and staff responsible for the release of HIV/STD data must take steps to prevent the identification of individuals.

5.0 Persons Affected

Person affected are DSHS employees and external entities that have access to HIV/STD surveillance, epidemiologic, public health follow-up and THMP data.

6.0 Responsibilities

The Local Responsible Party (LRP) is responsible for implementing and enforcing these data release guidelines. For the HIV/STD program, the managers of the HIV/STD Epidemiology and Surveillance Branch and the HIV/STD Comprehensive Services Branch are the LRP, each responsible for the proper release of the information originating from that program area. The HIV/STD Epidemiology and Surveillance Branch Manager will be responsible for the proper release of HIV/STD surveillance and epidemiologic data. The HIV/STD Comprehensive Services Branch Manager will be responsible for the proper release of THMP data and information. The LRP are jointly responsible for the proper release of public health follow-up data.

Regional programs and agencies contracting with the Program for surveillance or public health follow up must designate an LRP to oversee the release of HIV/STD data from their program. Regional programs and contractors that handle HIV/STD surveillance, epidemiologic, and public health follow-up data must develop a policy outlining guidelines for the release of local HIV/STD data or they may choose to adopt the HIV/STD Program's policy.

7.0 Data Release Guidelines

7.1 Aggregate Data

7.1.1 Fifty Rule

Aggregated HIV/AIDS and STD surveillance, epidemiologic, and public health follow-up data may be released if the underlying population consists of more than fifty people. Furthermore, the underlying population must be at least twice the number of cases. The size of the underlying population must be verified through the U.S. Census Bureau. Tables consisting of cells that do not satisfy the Fifty Rule are acceptable for release if those cells have been suppressed. Additional cells may also need to be suppressed to prevent the derivation of the suppressed data. Alternatively, data are acceptable for release if pooled to span a longer time period (i.e., 3 or 5 year periods). Another option is to collapse data categories if the data has been stratified by one or more categories, such as sex or age. All data at the zip code level or smaller and data that do not meet the fifty rule must be reviewed and approved for release by the DSHS HIV/STD Epidemiology and Surveillance Branch Manager. When population data are not available, the DSHS HIV/STD Epidemiology and Surveillance Branch Manager should be consulted.

7.1.2 Geographic Data

Data depicted on a map should be consistent with the aforementioned Fifty Rule. Geographic areas with populations that do not satisfy the Fifty Rule must be aggregated with data from one or more other geographic areas, although mapped data points with values of zero are acceptable for release.

The release of data in a map format created with GIS should not be accompanied by the individual layers and corresponding attribute tables used in the production of the map. The map should be released as a stand-alone image of a final product (e.g., JPEG format).

7.1.3 Medication Program Exception
The THMP may release aggregate program utilization and cost data without adherence to the Fifty Rule. Sub-county level data or stratified data must be reviewed and approved by the THMP manager or designee prior to release. All requests for THMP aggregate data will be processed by THMP staff and tracked by the THMP manager.

7.2 De-identified Individual Record-Level Data

The HIV/STD Program rarely releases de-identified individual record-level data. These data are only released for research or public health purposes, and these data shall only be released with a data sharing agreement in place and upon receiving approval from the LRP.

7.2.1 Geocoded Data
Individual record-level data consisting of geocoded address data for release in a map format or data file should not contain the geographic coordinates of addresses. Instead, individual addresses will identify the geographic level (e.g. county, census tract) to which they were geocoded.

7.2.3 Registry Matching
Confidential HIV/STD surveillance, epidemiologic, and public health follow-up data are routinely matched with data in other disease registries (e.g., cancer, tuberculosis) and data systems to improve data quality as a part of routine disease surveillance. HIV/AIDS and STD data may not be released to other programs for matching. Rather, the comparison of disease registries and other program data should be accomplished by the HIV/STD Program staff. The LRP is responsible for ensuring that data sharing agreements are in place when data are shared for matching purposes and are consistent with HIV/STD Program policies pertaining to the release of data.

7.3 Personally Identified Individual Record-Level Data

The HIV/STD Program strongly discourages the release of individual patient records that contain personal identifiers. In very limited circumstances, a patient's personal records may be released to providers, legal entities, and/or directly to the patient. The HIV/STD Program may also disclose individual patient data for public health purposes.

7.3.1 Patient Records
For requests through the HIV/STD Epidemiology and Surveillance Program, providers, patients and/or their lawyers may request only data relating to the patient. HIV/STD public health follow-up data will not be released to patients, providers, or legal entities under any circumstances, as those data contain partner information.

7.3.2 Public Health Purposes
Following routine matching of confidential HIV/STD surveillance, epidemiologic, and public health follow-up data with data in other disease registries, the HIV/STD Program may provide the other program with data on persons who are also diagnosed with an STD, including HIV. The LRP is responsible for ensuring that data sharing agreements are in place when data are shared and are consistent with HIV/STD Program policies pertaining to the release of data and maintaining confidentiality of the data.

7.3.3 THMP
Due to statutory provisions protecting the confidentiality of the manufacturers' drug pricing data (Federal Omnibus Budget Reconciliation Act of 1990 and in Section 340B of the Public Health Services Act, 42 U.S.C. 256B), drug pricing lists are considered restricted and cannot be released. Client records containing personal identifiers may be released to

treating physicians, servicing pharmacies, contractors, the patient, or other programs as necessary for the client to obtain services. THMP routinely shares THMP data with pharmacy benefit manager contractors, Medicare, and Medicaid. The LRP is responsible for ensuring that data sharing agreements or appropriate contracts are in place when THMP data are shared.

8.0 HIV/STD Program Procedures
HIV/STD Epidemiology, Surveillance and Public Health Follow-Up Data

8.1 Responding to Requests for Aggregated Data

Requests for data present an opportunity for direct interaction between the HIV/STD Program and our customers in the public, the media, the legislature, and other public health agencies. DSHS staff handling data requests should extend the most professional, courteous, accurate and rapid service available. The following procedure provides guidance for fulfilling data requests. DSHS recommends that regional and contracting programs create procedures for handling and tracking data requests that are similar.

Customers commonly initiate data requests via telephone or e-mails. An assigned staff member will work with the customer to complete the data request by clearly defining the specifics of the data requested. For requests of data that the HIV/STD Program does not have, program staff should refer the customer to other sources when possible. Key criteria for defining data requests may include:

- Disease(s) or diagnosis
- Reported cases versus diagnosed cases
- Number of cases, rates, or both
- Time period
- Geographic location(s)
- Demographic crosstabs (e.g., age, sex, race, risk group, etc) or restrictions (e.g., living cases, male cases, female cases, etc)
- Date the data request must be completed

Occasionally, the customer may not know how to define the data needed. In such cases, the assigned staff member may help define the request based on the question(s) the customer is trying to answer. For formal Public Information requests, assigned staff members are **not** permitted by state law to inquire about why the request is being made.

The assigned staff member will gather the customer's contact information, including e-mail address or fax number, in order to send the data. In general, assigned staff members should accept and meet the customer's deadline for receiving the data. If the deadline is unusually short, cannot be met, and/or another deadline cannot be negotiated, consult the LRP.

When completing data requests, assigned staff members should save the syntax and output files in a folder for future reference. These files are recorded in the data request tracking log to allow others to use or modify them for future requests. The requested data are most often saved in an electronic file format (e.g., Excel, Word, html, etc) and e-mailed to the customer. All data files should be clearly annotated, including titles and notes to thoroughly describe what the data represent. Additional notes should also be included to describe any special circumstances or limitations of the data, such as why some cells are suppressed.

If the data results are complete and follow the guidelines described in this policy, they may be sent to the customer along with the staff member's contact information.

If the data require further approval from the LRP due to issues with the data results, such as small underlying populations, then the results may only be sent upon approval. Staff must

not send questionable data through e-mail to the LRP for approval. Until it is approved, the data should be treated as confidential information and may not be e-mailed, even internally. Questionable data are to be hand-delivered.

8.2 Data Request Tracking

8.21 HIV/STD Surveillance Data

During and/or immediately following a request for data, the assigned staff member completing the request will document the request in the EpiDiv Request Log. Providing documentation of data requests in a centralized location allows the HIV/STD Program to quantify who its customers are and how they are being served. In addition, by identifying contact names and file information, future requests for repeat or similar data can be fulfilled more efficiently.

The Request Log is located on the public network in S:\Requests\Epidiv New Request Log.xls. Requests are organized by date. Select the appropriate tab for the year and scroll down to the month that the request was completed. Complete as many of the fields as possible.

8.2.2 Handling Requests from Special Customers

Staff should respond to requests from the media by following Policy Number AA-5007 (http://online.dshs.state.tx.us/policy/agency/aa%2D5036.htm).

All DSHS staff who receives a legislative contact should notify the appropriate Branch Manager immediately. Before responding to a legislative request, staff must obtain approval from appropriate Branch Manager prior to release of data. Immediately following the completion of a legislative request, a Legislative Contact Report should be e-mailed. At minimum, this report will be submitted to the assigned staff member's supervisor, the Branch Managers of the HIV/STD Epidemiology and Surveillance Branch and the Comprehensive Services Branch, the Unit Manager of the Epidemiology and Surveillance Unit, the Director of the Prevention and Intervention Section, the Assistant Commissioner for Prevention and Preparedness, the Office of Governmental Relations, and the individual responsible for legislative liaison at the Division of Prevention and Preparedness.

This report should contain the following information:

- Who made the request – which Legislator's office, contact person's name, telephone number and other contact information
- When the request was received
- What the question or issue was that prompted the request
- Summary of the response or copy of data released
- Any future follow-up required
- Name and contact information for the employee that responded to the request

Staff who receive an Open Records or Public Information Act request should follow Policy Number AA-5007 (http://online.dshs.state.tx.us/policy/agency/aa%2D5007.htm).

8.3 De-identified Data Requests

De-identified individual record-level data are only released upon approval by the LRP. Customers commonly initiate data requests via telephone or e-mail. For HIV/STD surveillance, epidemiologic, and public health follow-up data requests, customers must sign Data Release and Confidentiality Agreements prior to receipt of data. The Data Release and Confidentiality Agreements will specify:

- the permitted uses, disclosures, and final disposition of the data
- who is permitted to use or receive the data

- that the data recipient will use appropriate safeguards to prevent use or disclosure of the information outside that specified by the Data Release and Confidentiality Agreements

The dataset will be prepared by assigned staff and provided to the customer via secured means upon approval by the LRP. The LRP or designee will file the paperwork associated with the request and enter the request in the Data Release Tracking Log. The LRP or designee will provide the customer with a signed copy of the Data Release Agreement and must store hard copies of the agreement. Follow-up will be conducted with customers who receive individual record-level data to ensure that the data and any additional data files created have been properly destroyed on their stated project completion date.

All THMP data requests will be processed by THMP staff and tracked by the THMP manager.

External sites should develop and use their own data release agreement for local individual record-level requests, or the external sites may choose to use the DSHS Data Release Agreement.

Handling Requests for Research Purposes

Requests for individual record-level data from the HIV/STD Epidemiology and Surveillance Branch for research purposes must be reviewed and approved by the DSHS Institutional Review Board (IRB) and the Local Responsible Party. Procedures for submitting data requests to the DSHS IRB can be found at *http://www.dshs.state.tx.us/irb/default.shtm*. The requestor must also obtain approval from an IRB at the institution responsible for oversight of the research program. Prior to releasing datasets, all personal identifiers must be removed. Datasets that contain potentially identifying information must be maintained by the recipient in a manner consistent with the most current DSHS confidentiality and security guidelines regarding physical and electronic security. The staff of the research institution must comply with all security and confidential training requirements.

Upon approval by the IRBs, Data Release and Confidentiality Agreements must be signed prior to releasing the data (See Appendix A). The Data Release Agreement must specify the length of time that the research institution will maintain the data. All the data must be removed from all electronic files and hard copies at the conclusion of the timeframe specified in the Data Release Agreement. The research institution must provide documentation that these data have been destroyed in a confidential manner.
Requests for THMP individual record-level data for research purposes must be reviewed by the DSHS IRB.

8.4 Personally Identified Individual Record-Level Data

8.4.1 Requests From Legal Entities

Requests for individual HIV/STD surveillance, epidemiologic, or THMP patient records initiated via court orders, subpoenas, or legal counsel for a patient must be directed to the DSHS Office of General Counsel. Patients and/or their lawyers must sign a medical record release form before any data are released. The LRP must see the medical record release form and approve before data is released.

8.4.2 Requests by Patients or Providers

Providers requesting patient records or patients requesting their own records through the HIV/STD Epidemiology and Surveillance Branch must be directed to the DSHS Office of General Counsel. A medical record release form must be signed by the patients and the LRP must see the medical release form and approve before data is released. Requests for THMP client records do not need to be directed to the DSHS Office of General Counsel.

9.0 Revision History

Date	Action	Section
07/02/08	Extensive revision too numerous to list, therefore treated as new policy. Previously, this policy was numbered as 020.061	NA

HIV/STD Epidemiology and Surveillance Confidential Information Security Procedures	*Policy Number*	323.001
	Effective Date	July 3, 2008
	Revision Date	July 3, 2008
	Subject Matter Expert	Internal Workgroup
	Approval Authority	Branch Manager
	Signed by	Sharon K. Melville, MD, MPH

1.0 Purpose

This document establishes the general procedures that all HIV/STD surveillance and epidemiologic program staff, located in the Central Office and external sites, are required to follow concerning the collection, transmission, storage and maintenance of confidential information both in the office and in the field.

2.0 Definitions

Advanced Encryption Standard

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data.

Authorized User

Those individuals employed by the program who, in order to carry out their assigned duties have been granted access to confidential information.

Central Office

The HIV/STD Program, Department of State Health Services (DSHS) main office located in Austin Texas.

Confidential information

Any information which pertains to a patient that is intended to be kept in confidence or kept secret and could result in the identification of the patient should that information be released

Confidentiality

The ethical principle or legal right that a physician or other health professional or researcher will prevent unauthorized disclosure of any confidential information relating to patients and research participants

Encryption

The manipulation or encoding of information so that only parties intended to view the information can do so. There are many ways to encrypt information; most commonly available systems involve public key and symmetric key cryptography.

- A public key system uses a mathematically paired set of keys, a public key and a private key. Information encrypted with a public key can only be decrypted with the corresponding private key, and vice versa. Therefore, you can safely publish the public key, allowing anyone to encrypt a message that can be read only by the holder of the private key. Presuming that the private key is known to only one authorized individual, the message is then accessible only to that one individual.
- A symmetric key system is based on a single private key that is shared between parties. Symmetric systems require that keys be transmitted and held securely in order to be

effective, but are considered to be highly effective when the procedures are good and the number of individuals who possess the key is small. In general, the larger the key the more robust the protection.

Global Positioning Device (GPS)
A GPS is typically a hand-held or vehicle-mounted navigational system. It uses Global Positioning System (hence GPS) technology to triangulate any given position using three satellite signals relating to the unit.

Key-Card
A badge containing magnetically coded information, that when placed in the proximity of a reading device unlocks a door. Key cards are used as part of physical security systems.

Local Responsible Party (LRP)
An official who accepts responsibility for implementing and enforcing HIV/STD polices and procedures related to the security and confidentiality of HIV/STD surveillance, epidemiology, public health follow-up and medication program data and information. The LRP has the responsibility of reporting and assisting in the investigative breach process. A Local Responsible Party will be designated both internally and externally. Internally the HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch managers will be designated as the LRP.

Overall Responsible Party (ORP)
The official who accepts overall statewide responsibility for implementing and enforcing these security standards as they apply to HIV/AIDS surveillance data and who may be liable for breach of confidentiality. The state's security policy must indicate the ORP by name.

Password Protected
Files and directories that are protected from unauthorized access by requiring users to enter a password before access is allowed.

Personal Digital Assistants (PDA)
A PDA is a handheld computer, which has many uses, including, but not limited to: calculation, accessing the internet, sending and receiving e-mails, video recording, word processing, and Global Positioning (GPS).

Personal Identifier
A datum or collection of data which allows the possessor to determine the identity of a single individual with a specified degree of certainty; a personal identifier may permit the identification of an individual within a given database. Bits of data, when taken together, may be used to identify an individual. Personal identifiers may include name, address or place of residence, social security number, telephone number, fax number, and exact date of birth.

Removable Storage Device
A device that allows for the transportation of electronic information; there are many types of Removable Storage Devices including, but not limited to: USB port flash drives (memory sticks), diskettes, CD-ROMS, zip disks, tapes, smart cards, and removable hard drives.

External
Entities outside of the DSHS Central Office that the HIV/STD program contracts with or works in association with to conduct public health activities related to HIV/STD surveillance, epidemiology, public health follow-up and the medication program.

Secured Area
A confined physical space where HIV/STD data and information are located with entry limited to staff with authorized access; the secured area is usually defined by hard, floor-to-ceiling walls with a locking door and may include additional measures (e.g., alarms, security personnel).

Security
The protection of surveillance data and information systems, for the purposes of (1) preventing unauthorized release of identifying surveillance information or data from the systems (e.g., preventing a breach of confidentiality) and (2) protecting the integrity of the data by preventing accidental data loss or damage to the systems. Security includes measures to detect, document, and counter threats to the confidentiality or integrity of the systems.

Secure Voicemail
A Voice Mailbox system that is password protected and in which messages are stored on a protected network.

Surveillance
The ongoing and systematic collection, analysis and interpretation of health data in the process of describing and monitoring a health event; this information is used for assessing public health status, triggering public health action, defining public health priorities and evaluating programs.

Wi-Fi (Wireless Fidelity)
Refers to wireless network components that are based on one of the Wi-Fi Alliance's 802.11 standards. The Wi-Fi Alliance created the 802.11 standard so that manufacturers can make wireless products that work with other manufacturers' equipment. This equipment uses high-frequency radio waves rather than wires to communicate. Wi-Fi is commonly used to wirelessly access the Internet or a local network.

Wiki
A piece of server software that allows users to freely create and edit Web page content using any Web browser; Wiki supports hyperlinks and has simple text syntax for creating new pages and cross links between internal pages.

3.0 Physical Security

3.1 Buildings/Offices

- All surveillance and epidemiological confidential information, electronic and paper, must be maintained in a secure locked area with limited access. A secure area is an area which is protected by at least one level of physical security, although it is preferable that HIV information be maintained behind two levels of physical security. A security guard should not be the only level of security. Examples of physical security levels are:
    - Secured access card
    - Locked door
    - Reader code access
- The Local Responsible Party (LRP) for each site is responsible for approving the physical security levels of the site.
- The LRP for each site is responsible for maintaining a **log** which identifies all individuals with access to secured areas.

- Rooms containing confidential information must not have windows which could allow easy entry into the room.
- Keys, key-cards, and codes enabling access to secure areas as defined above must not be shared or loaned.
- Any secured area that allows access to visitors must have a process for tracking visitors' access.
- Visitors to secured areas must be escorted at all times.
- Persons with authorized access to secure areas must be able to identify visitors (e.g. Identification badge).
- Secured doors should not be propped open or disabled unless prior approval to do so has been obtained from the LRP.

3.2 Computer Workstations

- All computer workstations with access to confidential information must be in a secure area. A secure area is one in which there is at least one level of physical security, although it is preferable that computer workstations with access to HIV information be maintained behind two levels of physical security.
- Computer screens must not be readily observable by non-authorized users as they pass through the office area, sit at desks, or approach reception areas. Security screens may be installed on computer monitors to prevent viewing of information on the computer screen by anyone other than the operator.
- Computers used to access confidential information must be password protected at the Windows login level, and have a password protected screensaver program installed and activated.
- All network/computer passwords are to be at least eight characters in length and must be a combination of letters, characters and numbers, and not easily guessed.
- Network/computer passwords must expire based on current password guidelines.
- New or temporary passwords issued to a staff member must be changed upon receipt of the password.
- Computer passwords must not be shared with others.
- No one should access a computer or network using another person's access without written authorization.
- If a password's security is in doubt, it must be changed immediately.
- Passwords should not be written down but when necessary to do so, the stored passwords must be encrypted.
- Computer workstations must be locked (Ctrl/Alt/Delete - Lock Workstation) when a workstation is left unattended.
- Internet Control Message Protocol (ICMP) should not allow "Redirect Services" to devices (i.e. Blackberries) not authorized by the specific network administrators.
- Services running on the specific network should not allow "remote desktop" by individuals (i.e. computers) not in the network.
- Local hosting of servers (i.e. "wikis") on computers that contain confidential information is a security risk.
- Confidential data must not be accessed or worked with on any computer that is not secure.

4.0 Handling Paper Records

- When not in use, all documents with surveillance and epidemiological confidential information must be stored in a locked file cabinet in a locked secure area.
- Documents with confidential information should be returned to their secured storage after their use has been completed.
- Documents with confidential information must not be readily observable by non-authorized users as they pass through the office, sit at desks, or approach reception areas.
- When documents with confidential information are taken from a secured area they must be transported in a secure container (e.g. locked briefcase), not visible in a car, and must contain the minimum amount of confidential information necessary to do business and, where possible, must be coded to disguise any information that could easily be associated with HIV or AIDS and/or identity of the individual.
- Confidential information will be maintained and destroyed according to the DSHS records retention policy for surveillance and epidemiologic information or the local records retention policy.
- Documents with confidential information must be shredded using a shredder that is of commercial quality and has a crosscutting feature before disposing of them.
- Shredding of documents containing confidential information must be conducted by persons authorized to view the confidential information.
- Documents containing confidential information that are waiting to be shredded must be stored in a secure area.
- Stored documents with confidential information must be clearly marked as containing confidential information.
- Working with confidential surveillance and epidemiologic information at home (telecommuting) is prohibited.
- Confidential information will not routinely be taken to a private residence but if unavoidable then specific approval must be obtained from their supervisor or the LRP.
- Prior approval must be obtained from their supervisor or the LRP when business travel precludes the return of confidential surveillance information to the secured area by the close of business on the same day.

5.0 Telephone/Faxing/E-mail

5.1 Telephone (including cell phones)

- Telephone calls concerning confidential information must be made in an area where conversations cannot be **overheard**.
- Personnel must reasonably ascertain that phone contacts are legitimate before discussing confidential information on the phone.
- On the telephone, personnel will only share the minimum amount of confidential information needed to accomplish the surveillance or epidemiological objective of the call.
- Confidential information must never be left on voicemail systems unless they are secure systems (cell phone voice mail systems are generally not secure) or there is authorization from the call recipient to leave confidential information.
- Outgoing voicemail messages on telephones with non-secure voicemail, must ask the caller to leave only their name and number.
- Outgoing voicemail messages on telephones must not identify staff as being employed by the HIV/STD program.

- If a person is on a confidential call and they can hear other conversations over the line (often called cross talk) or experience similar issues, the conversation must end immediately and be reported to the LRP.

5.2 Faxing

- Facsimile transmission of confidential information must only be done when other methods of sending information are unavailable or would delay the timely provision of services.
- Confidential information sent using a facsimile must be faxed under a cover sheet. The cover sheet must not contain the words HIV, AIDS, or STD anywhere on it.
- The HIV/AIDS Reporting System (HARS) cityno and stateno are to be considered as identifying variables and should not be included on faxes.

- The information to be faxed must be
    - de-identified (client's name and all other identifying information removed) OR
    - the identifying information must be sent in a separate fax transmission only after the sender has confirmed receipt of the first fax with the receiver; OR
    - All HIV/STD related information has been removed or converted to a code
- Anyone sending a fax must confirm that the information faxed was received by the intended recipient
- Fax machines used to send or receive confidential information must be located in a secure area.
- Programs are encouraged to use separate fax machines instead of multifunctional machines which include faxing capabilities.

5.3 E-Mail

- E-mail transmissions, encrypted or non-encrypted, containing any confidential information must not be sent. The use of email attachments for the purpose of transmitting confidential information is prohibited (see Section V: Electronic Data Handling for methods of transmitting electronic data).
- The HARS cityno and stateno are to be considered as identifying variables and should not be included on emails or email attachments.
- Email and confidential information must not be accessed simultaneously to avoid accidental submission of data through this system. This includes any electronic device with internet capabilities.

6.0 Handling Confidential Mail

6.1 Incoming Mail

- All mail marked “confidential” must be checked by authorized personnel only and kept in a secured location until it is processed.
- Mail marked “confidential” should only be opened by the addressee.
- The person in charge of receiving the confidential mail must record the receipt of all mail into a log book, by the end of each day. Each log entry must note the name of the sender, what was received, and the date of receipt.
- The person in charge of receiving the confidential mail must contact the sender on the day of receipt to notify them that their mail was received.

6.2 Outgoing Mail

- All confidential HIV information sent using the mail system must be double enveloped. Confidential HIV information must first be first placed in a sealed, taped non-addressed envelope marked “CONFIDENTIAL”; that envelope is then placed in a second sealed and taped envelope marked “CONFIDENTIAL” and “TO BE OPENED BY ADDRESSEE ONLY.”
- All confidential STD (non-HIV) information sent using the mail system must be placed in a sealed, taped envelope that is marked “CONFIDENTIAL and “TO BE OPENED BY ADDRESSEE ONLY.” The envelope must contain the return address of the sender.
- The outer envelope must contain the return address of the sender. The words HIV/AIDS/STD must not appear in the body of the address or return address. This includes address stamps and/or pre-addressed envelopes.

7.0 Handling Electronic Data

7.1 Electronic Data Access

- Network drives, which contain confidential information, must have controls in place that enable only authorized users access.
- Staff **may not** attempt to access any data, program, or system for which they do not have approved authorization.

7.2 Electronic Data Storage

- Electronic data must be held in a technologically secure environment; the number of data repositories and the number of permitted users must be kept to a minimum.
- At the Central Office, all electronic confidential information must be stored on a secure password protected network drive on a “private computer.” A “private computer” is a computer which is not connected to the Internet, but is part of a DSHS network. The password for the secure drives, which contain confidential information, will only be given to authorized users.
- At external sites, all confidential information must either be stored on a computer which is not connected to a network (i.e. stand alone computer) or on a secure drive of a secure network (e.g. network with restricted access and/or firewall protection).
- No data is to be stored on the hard drive of any computer connected to a local or wide area network (WAN).
- When storing datasets, which are no longer in use, the dataset must be encrypted using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf) and stored either on a stand alone computer or on a secure drive.

7.3 Electronic Data Transmission

- Confidential electronic information being transferred between the Central Office and external sites, and between external sites, must be encrypted and transferred using secure networks approved by the LRP.
- Confidential information transmitted electronically between Central Office and external sites and between external sites, must be sent over the Health Alert Network (HAN)/Public Health Information Network (PHIN) as follows:
  1. Encrypt data on a secure drive using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197 and password protected. The password for the file must only be

shared with the recipient of the data and sent separately from the data. WinZip 9.0 or later can be used to encrypt the file.

2. Once the data has been encrypted, transfer the encrypted data from the secure drive to a location with access to the Health Alert Network.
3. Log in to the HAN/PHIN and upload your data.
4. Send an email to the person who will be receiving the file to inform them that the file has been uploaded; give them the encryption password.

- All confidential electronic data received by the Central Office from an external agency (e.g. electronic lab reports) will follow the same standards as those listed above.
- Surveillance and epidemiologic data must have personal identifiers removed (an analysis dataset) if taken out of the secured areas or accessed from an unsecured area.

8.0 Removable, External Storage Devices and Laptops

All staff that is authorized to access confidential information must be individually responsible for protecting their assigned/own laptop or other portable devices including, but not limited to: PDA, blackberries, cell phones, flash drives, diskettes, CD-ROMS, zip disks, tape backups, removable hard drives, smart cards, and/or GPS systems.

8.1 Laptops

- Confidential information **may not** be stored on the hard drive of a laptop computer. All confidential information must be encrypted, using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197, and stored on a removable storage device. The removable storage device containing the data must be separated from the laptop and stored in a secure location when not in use.
- When working with confidential information on a laptop computer, staff must ensure that unauthorized users cannot view the computer screen.
- Laptops used as a work computer fall under the same confidentiality and security guidelines as workstations (see physical security section).
- Laptops shall not be left unattended in non-secure areas. If you must leave a laptop in a room, the room must be locked or the laptop and other confidential information must be placed in a locked file cabinet.
- When traveling with a laptop, use a lockable carrying case for the laptop. If you do not have a lockable carrying case, a form-fitting padded sleeve for the laptop carried in a backpack, courier bag, briefcase, or other common nondescript carrying case may be used if approved by the LRP.
- When transporting a laptop, it is safer to rent or use a car with a locking trunk (not a hatchback/minivan/SUV). Regardless of vehicle type, laptops must never be visible from outside of the car.
- The laptop must always be locked up or stored in a locked file cabinet when it is not being used.
- Laptop and notebook computers with wireless connectivity capabilities (built-in or attached) must be disabled while working with confidential information.

8.2 Removable Storage Devices

- All confidential information placed on a removable storage device must be encrypted, using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197, and password protected. The password must be stored separately from the device.

- Any removable storage device containing confidential information is to be stored following the physical and electronic standards of this document.
- Removable storage devices containing confidential information must not be taken to a private residence unless specific permission has been granted by the LRP.
- Removable storage devices no longer in use must be destroyed.
- Acceptable methods of sanitizing diskettes and other storage devices that previously contained sensitive data include overwriting or degaussing (demagnetizing) before reuse. Alternatively, the diskettes and other storage devices may be physically destroyed (e.g., by incineration, shredding). Such physical destruction would include the device, not just the plastic case around the device.

8.3 Personal Storage Devices (PDA)/Blackberries/Cell Phones

- Security for PDA, blackberries, cell phone or any equivalent system will follow all electronic media and physical storage standards listed in this document.
- No confidential information will be stored on, or accessed from, a PDA, blackberry, cell phone or any equivalent system.
- PDA, blackberries, cell phone or any equivalent systems must be turned off when not in use.
- Functions of the PDA, blackberries, cell phone or any equivalent systems that are not immediately employed in the use of the system, (e.g. “Roaming”, “Text Messaging”, “Bluetooth”, photo capabilities) must be disabled.

9.0 Revision History

Date	Action	Section
07/03/08	This is a new procedure	

HIV/STD Public Health Follow-Up (PHFU) Confidential Information Security Procedures	*Policy Number*	322.001
	Effective Date	July 3, 2008
	Revision Date	July 3, 2008
	Subject Matter Expert	Internal Workgroup
	Approval Authority	Branch Manager
	Signed by Sharon K. Melville, MD, MPH	

1.0 Purpose

This document establishes the general procedures that all HIV/STD field and support staff, located in the DSHS regional and contract sites are required to follow concerning the collection, transmission, storage and maintenance of confidential information. See the HIV and STD Program Operating Procedures and Standards (POPS) (http://www.dshs.state.tx.us/hivstd/pops/default.shtm) for more information about PHFU associated with HIV-positive test results and general follow up practices and procedures.

2.0 Responsibilities

Disease Intervention Specialists (DIS) will not divulge the specific nature of his/her professional capacity to unauthorized persons in the course of disease intervention activities. Information gained in the course of work activity will not be divulged to unauthorized persons in any manner that may be construed to link an individual with a communicable disease. The DIS will handle each situation in a professional manner that safeguards the privacy of individuals.

3.0 Definitions

Advanced Encryption Standard

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data.

Authorized User

Those individuals employed by the program who, in order to carry out their assigned duties have been granted access to confidential information.

Central Office

The HIV/STD Program, Department of State Health Services (DSHS) main office located in Austin Texas.

Confidential Information

Any information which pertains to a patient that is intended to be kept in confidence or kept secret and could result in the identification of the patient should that information be released.

Confidentiality

The ethical principle or legal right that a physician or other health professional or researcher will prevent unauthorized disclosure of any confidential information relating to patients, and research participants

Encryption
The manipulation or encoding of information so that only parties intended to view the information can do so. There are many ways to encrypt information; most commonly available systems involve public key and symmetric key cryptography.

- A public key system uses a mathematically paired set of keys, a public key and a private key. Information encrypted with a public key can only be decrypted with the corresponding private key, and vice versa. Therefore, you can safely publish the public key, allowing anyone to encrypt a message that can be read only by the holder of the private key. Presuming that the private key is known to only one authorized individual, the message is then accessible only to that one individual.
- A symmetric key system is based on a single private key that is shared between parties. Symmetric systems require that keys be transmitted and held securely in order to be effective, but are considered to be highly effective when the procedures are good and the number of individuals who possess the key is small. In general, the larger the key the more robust the protection.

Global Positioning Device (GPS)
A GPS is typically a hand-held or vehicle-mounted navigational system. It uses Global Positioning System (hence GPS) technology to triangulate any given position using three satellite signals relating to the unit.

Key-Card
A badge containing magnetically coded information, when placed in the proximity of a reading device unlocks a door. Key cards are used as part of physical security systems.

Local Responsible Party (LRP)
An official who accepts responsibility for implementing and enforcing HIV/STD polices and procedures related to the security and confidentiality of HIV/STD surveillance, epidemiology, public health follow-up and medication program data and information. The LRP has the responsibility of reporting and assisting in the investigative breach process. An LRP will be designated both internally and externally. Internally the HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch managers will be designated as the LRP.

Password Protected
Files and directories that are protected from unauthorized access by requiring users to enter a password before access is allowed.

Personal Digital Assistants (PDA)
A PDA is a handheld computer, with many uses, including, but not limited to: calculation, accessing the internet, sending and receiving e-mails, video recording, word processing, and Global Positioning (GPS).

Personal Identifier
A datum or collection of data which allows the possessor to determine the identity of a single individual with a specified degree of certainty; a personal identifier may permit the identification of an individual within a given database. Bits of data, when taken together, may be used to identify an individual. Personal identifiers may include name, address or place of residence, social security number, telephone number, fax number, and exact date of birth.

Removable Storage Device
A device that allows for the transportation of electronic information; there are many types including, but not limited to: USB port flash drives (memory sticks), diskettes, CD-ROMS, zip disks, tapes, smart cards, and removable hard drives.

External
Entities outside of the DSHS Central Office that the HIV/STD program contracts with or works in association with to conduct public health activities related to HIV/STD surveillance, epidemiology, public health follow-up and the medication program.

Secured area
A confined physical space where HIV/STD data and information are located with entry limited to staff with authorized access; the secured area is usually defined by hard, floor-to-ceiling walls with a locking door and may include additional measures (e.g., alarms, security personnel).

Security
The protection of surveillance data and information systems, for the purposes of (1) preventing unauthorized release of identifying surveillance information or data from the systems (e.g., preventing a breach of confidentiality) and (2) protecting the integrity of the data by preventing accidental data loss or damage to the systems. Security includes measures to detect, document, and counter threats to the confidentiality or integrity of the systems.

Secure Voicemail
A Voice Mailbox system that is password protected and in which messages are stored on a protected network.

Surveillance
The ongoing and systematic collection, analysis and interpretation of health data in the process of describing and monitoring a health event; this information is used for assessing public health status, triggering public health action, defining public health priorities and evaluating programs.

Wi-Fi (Wireless Fidelity)
Refers to wireless network components that are based on one of the Wi-Fi Alliance's 802.11 standards. The Wi-Fi Alliance created the 802.11 standard so that manufacturers can make wireless products that work with other manufacturers' equipment. This equipment uses high-frequency radio waves rather than wires to communicate. Wi-Fi is commonly used to wirelessly access the Internet or a local network.

Wiki
A piece of server software that allows users to freely create and edit Web page content using any Web browser; Wiki supports hyperlinks and has simple text syntax for creating new pages and crosslink between internal pages.

4.0 Physical Security

4.1 Buildings/Offices

- All confidential information, electronic and paper, must be maintained in a secure area. A secure area is an area which is protected by at least one level of physical security, although it is preferable that HIV/STD information be maintained behind two levels of physical security. Examples of physical security levels are:
    - Secured access card reader access
    - Locked door
    - Security guard
- The Local Responsible Party (LRP) for each site is responsible for approving the physical security levels of the site.
- The LRP for each site is responsible for maintaining a **log** that identifies all individuals with access to secured areas.
- Rooms containing confidential information should not have windows that could allow easy entry into the room.
- Keys, key-cards and codes enabling access to secured facilities must not be shared or loaned.
- Any secured area that allows access to visitors must have a process for tracking visitors' access.
- Visitors to secured areas must be escorted at all times.
- Persons with authorized access to secure areas must be able to identify visitors (e.g. DSHS or local badge).
- Secured doors should not be propped open or disabled unless prior approval of the LRP has been obtained.

4.2 Computer Workstations

- All computer workstations with access to confidential information must be in a secure area. A secure area is one in which there is at least one level of physical security, although it is preferable that computer workstations with access to HIV/STD information be maintained behind two levels of physical security.
- Computer screens must not be readily observable by non-authorized users as they pass through the office area, sit at desks or approach reception areas.
- Computers used to access to confidential information must be password protected at the Windows login level.
- All network/computer passwords are to be at least eight characters in length and must be a combination of letters, characters and numbers, and not easily guessed.
- Network/computer passwords must expire based on current password guidelines.
- New or temporary passwords issued to a staff member must be changed upon receipt of the password.
- Computer passwords must not be shared with others.
- No one should access a computer or network using another person's access without written authorization.
- If a password's security is in doubt, it must be changed immediately.
- Stored passwords must be encrypted.
- Computer workstations must be locked (Ctrl/Alt/Delete - Lock Workstation) when a workstation is left unattended.

- Internet Control Message Protocol (ICMP) should not allow “Redirect Services” to devices (i.e. Blackberries) not authorized by the specific network administrators.
- Services running on the specific Network should not allow "remote desktop" by individuals (i.e. computers) not in the network.
- Local hosting of servers (i.e. “wikis”) on computers that contain confidential information is a security risk.
- Confidential data must not be accessed or worked with on any computer that is not secure.

5.0 Handling Paper Records

5.1 In the Office

- When not in use, all documents with confidential information must be stored in a locked file or locked room in a secure area.
- Documents with confidential information must not be readily observable by non-authorized users as they pass through the office, sit at desks or approach reception areas.
- When documents with confidential information are taken from a secured area within the work space they must contain the minimum amount of confidential information necessary to do business and, where possible, must be coded to disguise any information that could easily be associated with HIV/STD and/or identity of the individual.
- Documents with confidential information should be returned to their secured storage immediately after their use has been completed.
- Confidential information will be maintained and destroyed according to the DSHS records retention policy for field record information or the local records retention policy.
- Documents with confidential information must be shredded using a shredder that is of commercial quality and has a crosscutting feature before disposing of them.
- Stored documents with confidential information must be clearly marked as containing confidential information.
- Confidential documents to be shredded, must either be under the direct control of the staff member, or placed in a designated container labeled “confidential material to be shredded” in a secure area.
- Copies of a Field Record will not be made for any unauthorized purpose.
- Removing Interview Records from the workplace is prohibited.
- The existence or contents of the Interview Record will not be divulged to any unauthorized persons.
- Completed copies of the Interview Record will not be destroyed except as directed by the supervisor and in the manner described for the Field Record.

5.2 Outside the Office

- Workers should take only confidential information that will be immediately used from a secured area.
- Confidential information will not be left unattended in any place or area to which unauthorized persons may reasonably gain access. If a Field Record is lost, the matter is reported to the supervisor immediately.

- Confidential information (field records) will not be taken to a private residence, place of business, or any other location outside a DIS' vehicle other than their own home.
- When documents with confidential information (e.g., field records, test results to be provided to a client) are taken from a secured area to the field they must contain the minimum amount of confidential information necessary to do business and, where possible, must be coded to disguise any information that could easily be associated with HIV/STD.
- The contents of the Field Record will not be divulged to any unauthorized persons. If investigative records are taken into the field, they will be carried in a way to insure against being lost or displayed in any way. The Field Records will be properly coded and code sheets will not be kept in the pouch

6.0 Telephone/Faxing/Email

6.1 Telephone (including cell phones)

- Telephone calls concerning confidential information must be made in an area where conversations cannot be **overheard**.
- Personnel must reasonably ascertain that phone contacts are legitimate before discussing confidential information on the phone.
- On the telephone, personnel will only share the minimum amount of information to accomplish PHFU
- The sharing of specific information about individuals with an authorized person will be done according to local policies and only after taking reasonable precautions to confirm the identity of the authorized person.
- Laboratory test results may be furnished to clients over the telephone in accordance with local policies and safeguards. This includes notifying clients of a negative HIV test result. HIV positive results will not be divulged by telephone.
- Confidential information must never be left on voicemail systems unless they are secure systems or there is authorization (verbal or written) from the call recipient to leave confidential information.
- Outgoing voicemail messages on telephones with non-secure voicemail, must ask the caller to only leave their name and number.
- Outgoing voicemail messages on telephones must not identify staff as being employed by the HIV/STD program.
- If a person is on a confidential call and they can hear other conversations over the line (often called cross talk) or experience similar issues, the conversation must be ended immediately and reported to the LRP.

6.2 Faxing

- Facsimile transmission of confidential information must only be done when other methods of sending information are unavailable or would delay the timely provision of services.
- Confidential information sent using a facsimile must be faxed under a cover sheet. The cover sheet must not contain the words HIV, AIDS, or STD anywhere on it.

- The information to be faxed must be:
    - de-identified (client's name and all other identifying information removed) OR
    - the identifying information must be sent in a separate fax transmission only after the sender has confirmed receipt of the first fax with the receiver; OR
    - All HIV/STD related information has been removed or converted to a code
- Senders of faxes will confirm that the information faxed was received by the intended recipient
- Fax machines used to send or receive confidential information must be located in a secure area.
- Programs are encouraged to use separate fax machines instead of multifunctional machines which include faxing capabilities.

6.3 Email

- E-mail transmissions, encrypted or non-encrypted, containing any confidential information must not be sent. The use of email attachments for the purpose of transmitting confidential information is prohibited (see Section V: Electronic Data Handling for methods of transmitting electronic data). Note: this does not include emails sent using the **Internet Contact Policy** set forth in Attachment 'A' of Chapter 6 of the POPS since no confidential information is contained in the e-mail. http://www.dshs.state.tx.us/hivstd/pops/POPS.doc#chapter6
- Emails following the Internet Contact Policy may be sent by HIV/STD program staff as part of PHFU. This also encompasses PHFU through chat room contact. The procedures for accomplishing this in a confidential manner are set forth in the above-mentioned attachment.
- Email and confidential information must not be accessed simultaneously to avoid accidental submission of data through this system. This includes any electronic device with internet capabilities.

7.0 Handling Confidential Mail.

- All HIV/STD referrals sent using the mail system must be placed in a sealed envelope that is marked "CONFIDENTIAL."
- The envelope must contain the return address of the sender. The words HIV/AIDS/STD must not appear in the body of the address or return address. This includes any address stamps and/or pre-addressed envelopes.

8.0 Handling Electronic Data

8.1 Electronic Data Access

- Network drives that contain confidential information must have controls in place that only enable only authorized users' access.
- Staff **may not** attempt to access any data, program, or system for which they do not have approved authorization.

8.2 Electronic Data Storage

- Electronic data must be held in a technologically secure environment; the number of data repositories and the number of permitted users must be kept to a minimum.
- At the Central Office, all electronic confidential information must be stored on a secure password protected network drive on a "private computer." A "private computer" is a computer that is not connected to the Internet, but is part of a DSHS network. The password for the secure drives, which contain confidential information, will only be given to authorized users.
- At external sites, all confidential information must either be stored on a computer that is not connected to a network (i.e. stand alone computer) or on a secure drive of a secure network (e.g. network with restricted access and/or firewall protection).
- No confidential data are to be stored on the hard drive of any computer connected to a local or wide area network.
- When storing datasets that are no longer *in use, the dataset must be encrypted using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf) and stored either on a stand alone computer or on a secure drive.*

8.3 Electronic Data Transmission

- Confidential electronic information being transferred between the Central Office and external sites, and between external sites, must be encrypted and transferred using secure networks.
- Confidential information transmitted electronically between Central Office and external sites and between external sites, must be sent over the Health Alert Network (HAN)/Public Health Information Network (PHIN) as follows:
    1. Encrypt data on a secure drive using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197 and password protected. The password for the file must only be shared with the recipient of the data and sent separately from the data. WinZip 9.0 or later can be used to encrypt the file.
    2. Once the data has been encrypted, transfer the encrypted data from the secure drive to a location with access to the Health Alert Network.
    3. Log in to the HAN/PHIN and upload your data
    4. Send an email to the person who will be receiving the file to inform them that the file has been uploaded; give them the encryption password

9.0 Removable External Storage Devices and Laptops

All staff that are authorized to access confidential information must be individually responsible for protecting their assigned/own laptop, or other portable devices including, but not limited to: PDA, blackberries, cell phones, flash drives, diskettes, CD-ROMS, zip disks, tape backups, removable hard drives, smart cards, and/or GPS systems.

9.1 Laptops

- Confidential information **may not** be stored on the hard drive of a laptop computer. All confidential information must be encrypted, using encryption

software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197, and stored on a removable storage device. The removable storage device containing the data must be separated from the laptop and stored in a secure location when not in use.

- When working with confidential information on a laptop computer, staff must ensure that no unauthorized users can view the computer screen.
- Laptops used as a work computer fall under the same confidentiality and security guidelines as workstations (see physical security section).
- Laptops shall not be left unattended in non-secure areas. If you must leave a laptop in a room, the room must be locked or the laptop and other confidential information must be placed in a locked file cabinet.
- When traveling with a laptop, use a lockable carrying case for the laptop. If you do not have a lockable carrying case, a form-fitting padded sleeve for the laptop carried in a backpack, courier bag, briefcase, or other common nondescript carrying case may be safer.
- When transporting a laptop, it is safer to rent or use a car with a locking trunk (not a hatchback/minivan/SUV). Regardless of vehicle type, laptops must never be visible from outside of the car.
- The laptop must always be locked up or stored in a locked file cabinet when it is not being used.
- Laptop and notebook computers with wireless connectivity capabilities (built-in or attached) must be disabled while working with confidential information.

9.2 Removable Storage Devices

- All confidential information placed on a removable storage device must be encrypted, using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197, and password protected. The password must be stored separately from the device.
- Any removable storage device containing confidential information is to be stored following the physical and electronic standards of this document.
- Removable storage devices containing confidential information must not be taken to a private residence unless specific permission has been granted by the LRP.
- Removable storage devices no longer in use must be destroyed.
- Acceptable methods of sanitizing diskettes and other storage devices that previously contained sensitive data include overwriting or degaussing (demagnetizing) before reuse. Alternatively, the diskettes and other storage devices may be physically destroyed (e.g., by incineration, shredding). Such physical destruction would include the device, not just the plastic case around the device.

9.3 Personal Storage Devices (PDA)/Blackberries/Cell Phones

- Security for PDA, blackberries, cell phone or any equivalent system will follow all electronic media and physical storage standards listed in this document.
- No confidential information will be stored on, or accessed from, a PDA, blackberry, cell phone or any equivalent system.
- Functions of the PDA, blackberries, cell phone or any equivalent systems that are not immediately employed in the use of the system (e.g. “Roaming”, “Text messaging”, “Bluetooth”, photo capabilities) must be disabled.

9.4 GPS systems

- Staff is responsible for ensuring that their GPS systems are secured from damage and/or theft.
- Staff is responsible for ensuring that the address information entered into these systems cannot be linked in any way with the HIV/STD client.

10.0 Revision History

Date	Action	Section
07/03/08	This is a new procedure	

TEXAS Department of State Health Services	*Policy Number*	300.001
	Effective Date	July 2, 2008
	Revision Date	July 2, 2008
	Subject Matter Expert	Special Projects
Overall Responsible Party for HIV/AIDS Surveillance Data	*Approval Authority*	Branch Manager
	Signed by	Sharon K. Melville, MD, MPH

1.0 Purpose
The purpose of this document is to provide for a clear line of responsibility in the area of data security and the maintenance of confidential HIV/AIDS surveillance information.

2.0 Definitions
Overall Responsible Party (ORP) – a public official with sufficient authority to make decisions about statewide HIV/AIDS surveillance operations; the ORP is responsible for the security and confidentiality of the HIV/AIDS surveillance system.

3.0 Background
The Centers for Disease Control and Prevention (CDC) HIV/AIDS Surveillance Cooperative Agreement and the CDC HIV/AIDS Surveillance Security and Confidentiality Guidelines require each grantee to have a policy in place that names the individual who is the ORP.

4.0 Authority
CDC Technical Guidance for HIV/AIDS Surveillance Programs (Atlanta, GA 2006)

5.0 Policy
Sharon K. Melville, MD, MPH, Manager, HIV/STD Epidemiology and Surveillance Branch, Department of State Health Services, is the ORP for the state of Texas.

6.0 Responsibilities
The ORP has responsibility for the security of the surveillance system (including processes, data, information, software, and hardware) and may have liability for any breach of confidentiality. The ORP is responsible for determining how surveillance information will be protected when it is collected, stored, analyzed, released, and dispositioned.

7.0 Procedures
The name of the individual, who is designated as the ORP, rather than an organizational position, must be provided to CDC annually.

8.0 Revision History

Date	Action	Section
April 1, 2008	This is a new policy	n/a

HIV/STD Confidential Information Security Policy	*Policy Number*	301.001
	Effective Date	July 2, 2008
	Revision Date	July 2, 2008
	Subject Matter Expert	Surveillance Specialist
	Approval Authority	Branch Manager
	Signed by	Sharon K. Melville, MD, MPH

1.0 Purpose

The purpose of this policy is to define security standards for protecting the confidential information collected and maintained by the HIV/STD program associated with surveillance, epidemiology, public-health follow-up, and the Texas HIV Medication Program. This policy addresses the administrative, physical, and technical safeguards for the security of confidential information.

This policy has been written in alignment with requirements in the Department of State Health Services (DSHS) *HIV and STD Program Operating Procedures and Standards (POPS)* (http://www.dshs.state.tx.us/hivstd/pops/default.shtm), the DSHS IR-2204 Information Security Policy **(**http://online.dshs.state.tx.us/it/standards/securitystd.htm), Computer Usage Policy IR-2202, the Centers for Disease Control and Prevention's (CDC) Program Operations Guidelines for STD Prevention, (http://www.cdc.gov/std/Program/overview/TOC-PGoverview.htm), and the CDC's *Technical Guidance for HIV/AIDS Surveillance Programs* (Atlanta, GA; 2006), wherever possible and/or appropriate.

2.0 Background

In fulfilling its mission to prevent, treat and control the spread of HIV, STDs and other communicable diseases, the DSHS HIV/STD program, its contractors and external partners obtain personal and private information regarding individuals they serve. The HIV/STD program must be vigilant in maintaining the integrity of the systems that contain this information.

3.0 Authority

V.T.C.A., Penal Code, Chapter 16, Chapter 33; V.T.C.A. Health and Safety Code, 81.046 and 81.103-81.104; V.T.C.A., Texas Government Code, Chapter 552

4.0 Definitions

Central Office: The HIV/STD Program, Department of State Health Services (DSHS) main office located in Austin Texas.

Confidential information: Any information which pertains to a patient that is intended to be kept in confidence or kept secret and could result in the identification of the patient should that information be released.

Confidentiality: The ethical principle or legal right that a physician or other health professional or researcher will prevent unauthorized disclosure of any confidential information relating to patients, and research participants.

Local Responsible Party (LRP): An official who accepts responsibility for implementing and enforcing HIV/STD polices and procedures related to the security and confidentiality of HIV/STD surveillance, epidemiology, public health follow-up and medication program data and information. The LRP also has the responsibility of reporting and assisting in the investigative breach process.

A Local Responsible Party will be designated both internally and externally. Internally the HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch managers will be designated as the Local Responsible Parties.

External: Entities outside of the DSHS Central Office that the HIV/STD program contracts with or works in association with to conduct public health activities related to HIV/STD surveillance, epidemiology, public health follow-up and the medication program.

Security: The protection of surveillance data and information systems for the purposes of (1) preventing unauthorized release of identifying surveillance information or data from the systems (e.g., preventing a breach of confidentiality) and (2) protecting the integrity of the data by preventing accidental data loss or damage to the systems. Security includes measures to detect, document, and counter threats to the confidentiality or integrity of the systems.

5.0 Policy

It is the policy of the DSHS HIV/STD Program that information collected to prevent, treat, and control the spread of HIV and STDs will be protected and maintained to ensure patient confidentiality.

6.0 Persons Affected

This policy applies to all persons who may have access to confidential HIV/STD information associated with surveillance, epidemiology, public health follow up, and the Texas HIV Medication Program. This includes DSHS HIV/STD Program employees (permanent and temporary), IT staff, volunteers, students, and DSHS HIV/STD Program contractors.

7.0 Responsibilities

All persons affected by this policy (specified in section 6.0) are required to follow this policy and the relevant procedures associated with this policy.

- All persons must complete the following before being given access to confidential information:
    - Sign a confidentiality agreement that affirms individual responsibility for keeping client information and data confidential. The original must be stored in the employee's personnel file and a copy must be maintained by the employee. The confidentiality agreement must be signed annually.
    - Sign an assurance that they have reviewed HIV/STD Program security policies and procedures relevant to their position.
    - Successfully complete confidentiality and security training. The date(s) of the training(s) must be documented in the employee's personnel file. For DSHS employees, this training will be in addition to the security awareness and security/computer usage training required by DSHS policy

- All persons are individually responsible for ensuring that the confidential information they work with is protected. This responsibility includes protecting all passwords, keys, and codes that enable access to confidential information.

- All persons are responsible for reporting possible security risks to the LRP.

- All persons are individually responsible for protection of his/her own desk/work area, workstation, laptops or other devices associated with confidential information.

- All persons are responsible for challenging those persons who are not authorized to access confidential information.

- Confidential information gained in the course of work activity will not be divulged to unauthorized persons.

- Upon resignation or termination, all confidential information and keys or devices that enable access to physical and electronic locations where confidential information may be stored must be returned to his/her immediate supervisor.

Local Responsible Party

- All external sites and the Central Office must designate a Local Responsible Party (LRP).
- Internally the HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch managers will be designated as the Local Responsible Parties.
- The LRP will approve any HIV/STD program staff requiring access to confidential information maintained by the HIV/STD Program. The LRP will grant authorization to persons who have a work-related need to view confidential information.
- The LRP will ensure that all staff, including contractors, are trained as specified in the training requirements listed at (HIV/STD Security Training Plan) and as otherwise specified by DSHS.
- The LRP will maintain a list of persons who have been granted authorization to view and work with confidential information. The LRP will review authorized user lists annually.
- The LRP will ensure that this policy is reviewed annually and that evolving technology is reviewed on an on-going basis to make certain that the program's data remains as secure as possible.
- The LRP will be responsible for re-evaluating and re-assigning access to confidential information when an employee changes position within the HIV/STD program.

8.0 Procedures

All external programs must maintain written procedures for maintaining the security of confidential information. Such procedures must include the elements listed in the applicable activity-specific procedures for HIV/STD Surveillance, Public Health Follow-Up, the Medication Program and the Medical Monitoring Project.

9.0 Revision History

Date	Action	Section
07/02/08	This is a new policy	

TEXAS Department of State Health Services	*Policy Number*	303.001
	Effective Date	February 10, 1999
	Revision Date	July 2, 2008
	Subject Matter Expert	Surveillance Specialist
	Approval Authority	Branch Manager
HIV/STD Breach of Confidentiality Response Policy	*Signed by* Sharon K. Melville, MD, MPH	

1.0 Purpose

This policy describes the actions required of the Texas Department of State Health Services (DSHS) HIV/STD Program and entities with whom DSHS has a contractual or professional relationship to handle confidential HIV/STD surveillance, epidemiological, medication, and public health follow-up data in the event of a suspected breach. This policy also outlines how to address negligent or purposeful release of confidential client information.

This policy has been written to align with requirements in the Department of State Health Services (DSHS) *HIV and STD Program Operating Procedures and Standards (POPS)* (http://www.dshs.state.tx.us/hivstd/pops/default.shtm), the DSHS IR-2204 Information Security Policy (http://online.dshs.state.tx.us/it/standards/securitystd.htm), the Centers for Disease Control and Prevention's (CDC) Program Operations Guidelines for STD Prevention (http://www.cdc.gov/std/Program/overview/TOC-PGoverview.htm), and the CDC's *Technical Guidance for HIV/AIDS Surveillance Programs* (Atlanta, GA; 2006), wherever possible and/or appropriate.

2.0 Background

In fulfilling its mission to prevent, treat, and control the spread of HIV, STDs and other communicable diseases, the DSHS HIV/STD program, its contractors and external partners obtain confidential information regarding individuals they serve. These individuals trust that the HIV/STD program will take every precaution to protect that information in order to retain their confidentiality. The HIV/STD program must be vigilant in maintaining the integrity of systems that contain this confidential information.

3.0 Authority

Vernon's Texas Statutes and Codes Annotated (V.T.C.A.), Penal Code, Chapter 16, Chapter 33; V.T.C.A. Health and Safety Code, 81.046 and 81.103-81.104; V.T.C.A., Texas Government Code, Chapter 552

4.0 Definitions

Breach of Confidentiality- A breach of protocol that results in the improper disclosure of confidential information. The result is confidential information being: 1) accidentally or purposefully released verbally, electronically, or by paper medium, to an entity or person that by law does not have a right or need to know, or 2) purposefully accessed either in person or electronically by an entity or person that by law does not have a right or need to know.

Breach of Protocol - A departure from the established policies and procedures that may result in the improper disclosure of confidential information; an infraction or violation of a standard or obligation. This includes any unauthorized use of data, including de-identified data.

Central Office- The HIV/STD Program, Department of State Health Services (DSHS) main office located in Austin Texas.

Confidential Information- Any information which pertains to a patient that is intended to be kept in confidence or kept secret and could result in the identification of the patient should that information be released. and.

Confidentiality- The ethical principle or legal right that a physician or other health professional or researcher will prevent unauthorized disclosure of any confidential information relating to patients and research participants..

External- Entities outside of the DSHS Central Office that the HIV/STD program contracts with or works in association with to conduct public health activities related to HIV/STD surveillance, epidemiology, public health follow-up and the medication program.

Internal- Refers to staff and occurrences located at DSHS Central Office in Austin, Texas.

Local Responsible Party (LRP)**-** An official who accepts responsibility for implementing and enforcing HIV/STD security and confidentiality polices and procedures related to HIV/STD surveillance, epidemiology, public health follow-up and medication program data and information and has the responsibility of reporting and assisting in the investigative breach process.

Negligence- The failure to use reasonable care. The failure to do (or not to do) something that a reasonably prudent person would do (or not do) under like circumstances. A departure from what an ordinary reasonable member of the community would do in the same community. Negligence is a 'legal cause' of damage if it directly, and in natural and continuous sequence, produces or contributes substantially to loss, injury, or damage, so it can reasonably be said that if not for the negligence, the loss, injury, or damage would not have occurred.

Purposeful-Deliberate and with the intention to cause harm to another.

Security Officer- Internally, the individual designated by each group in the HIV/STD program to be part of the Security Team. The Security Officer assists in the investigative process of reported suspected breaches when the incident is directly related to the security officer's program (group) area.

Security Team- Internally, the Security Team consists of a security officer, group manger, and the Local Responsible Party. Externally, this team consists of appropriate staff designated to serve in this team. The Security Team is responsible for investigating suspected breaches, gathering all facts related to the incident, drawing conclusions, making recommendations for further action, and providing a closing report.

Suspected Breach: An alleged infraction or violation of a standard that may result in unauthorized disclosure of confidential information

5.0 Policy

The DSHS HIV/STD program ensures that appropriate DSHS staff members will respond to suspected breaches by reporting, investigating and providing follow-up to these incidents. This policy prescribes guidelines for addressing deviations from the established policies and procedures as specified in the DSHS HIV/STD Confidential Information Security Policy and the Release of HIV/AIDS and STD Data Policy.

6.0 Persons Affected/Applicability

This policy applies to all DSHS employees, IT staff, temporary employees, volunteers, students, DSHS program contractors, and any other persons who could potentially view and/or have access to HIV/STD confidential information.

7.0 Responsibilities

All persons affected by this policy, as specified in section 6.0, are responsible for the reporting of suspected breaches.

Internal and external sites are responsible for designating a Local Responsible Party (LRP). Internally the HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch Managers will be designated as the LRPs. The HIV/STD Epidemiology and Surveillance Branch Manager will be responsible for investigating and responding to breaches related to HIV/STD surveillance and epidemiological data and information. The HIV/STD Comprehensive Services Branch Manager will be responsible for investigating and responding to breaches related to medication data and information. The HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch managers will be jointly responsible for investigating and responding to breaches related to public health follow-up information and data. The LRP will be responsible for implementing and enforcing security and confidentiality polices and procedures and for investigating suspected breaches.

Internal and external sites are responsible for designating a Security Team. The Security Team will be responsible for assisting the LRP investigate suspected breaches, gather all facts related to the incident, draw conclusions, make recommendations for further action, and provide a closing report.

8.0 Reporting and Investigating a Suspected Breach

Internally, the DSHS HIV/STD Program will create and identify a Security Team, procedure, and documents for tracking, reporting, and investigating suspected breaches. Internally, the Security Team consists of a security officer, group manger, and the LRP. The group manager and the Security Officer will assist in the investigative process of reported suspected breaches when the incident is directly related to their respective program (group) area. When reporting a suspected breach, confidential patient information will not be submitted on the DSHS HIV/STD Program breach reporting form. In response to a suspected breach, the DSHS HIV/STD Program will follow internal procedures for reporting, documenting and investigating the incident. If a suspected breach has not been identified but confidential information is potentially at risk of being divulged, the LRP will be notified directly. The breach report form will not be used in these instances.

Externally, policies and procedures that are consonant with the DSHS HIV/STD Program policy for documenting, investigating, and reporting suspected breaches will be created. External sites will designate an LRP and a Security Team responsible for reporting and investigating a suspected breach. Externally, the Security Team consists of appropriate staff designated to serve in this team. The external LRP will inform the appropriate internal LRP of a suspected breach within 24 hours after the incident is first reported.

8.1 Action Steps in Response to a Suspected Breach

Internally, the DSHS HIV/STD Program will follow established procedures for responding to a suspected breach. The Security Team will be responsible for determining the validity of a suspected breach and determining the type of breach that has occurred. Recommended corrective actions will be taken based on the type of breach determined to have occurred.

Externally, regional and contracting offices will implement policies and procedures that adhere to the guidelines set forth in the DSHS HIV/STD Program policy for responding to suspected breaches. The external LRP will communicate the Security Team's recommended corrective actions to the appropriate internal LRP. Recommended corrective actions will be based on local personnel policies for dealing with employees who violate protocols and/or confidentiality. Once the external and internal LRPs are in agreement with the proposed recommendations, the external LRP will be responsible for providing a final closing report to the internal LRP. However, when a response to a confirmed breach is deemed insufficient by the internal LRPs, DSHS may place the DSHS contracted site on sanctions as referenced in Policy AA-5116 (Sanctions and Remedies for Contract Non-Compliance) http://online.dshs.state.tx.us/policy/agency/aa-5116.htm

8.2 Follow-up to a Breach and Maintenance of Files

Internally, the DSHS HIV/STD Program will follow established procedures requiring follow-up to a confirmed breach. In the event of a confirmed breach, the Group Manager is responsible for providing monthly follow-up reports to the LRP documenting progress on the corrective action plan. Monthly follow-up reports will be submitted until corrective actions are concluded or deemed sufficient by the internal LRP. Subsequently, all hard copies of final reports and electronic data will be maintained by the HIV/STD Epidemiology and Surveillance Branch Overall Responsible Party (ORP) and/or designee(s) as outlined in the DSHS HIV/STD Program policies and procedures.

External sites will adopt policy and procedures requiring follow-up to a confirmed breach that meet the guidelines of the DSHS HIV/STD Program policy and procedures. The external LRP will be responsible for providing monthly follow-up reports to the appropriate internal LRP until corrective actions are concluded or deemed sufficient by the internal LRP. The DSHS HIV/STD Program will maintain breach-reporting forms of suspected breaches in the DSHS contractor file. Breach reporting forms that are kept with the DSHS contractor file will be redacted of any confidential information pertaining to the person who committed the suspected breach.

To prevent further breaches in protocol, internal and external sites involved in handling confidential information will be thoroughly retrained on the policies of the agency and the program. As part of the training, examples should be given to illustrate what constitutes a breach and describe the consequences if someone releases confidential information. It should be stressed that the individual and the agency may be held liable for breaches.

9.0 Procedures-Internal

Reporting a Suspected Breach

1.	The DSHS staff member who receives the initial notice of the suspected breach will document the incident using the Breach Report Form ("Section 1: Initial Report").
2.	The initial part of the breach report must be completed and submitted via e-mail to the appropriate Group Manager, within 24 hours of the incident. If the Group Manager is not available, then the acting Group Manager is notified via e-mail within 24 hours of the incident.
3.	The DSHS staff person must receive an e-mail confirmation from the Group Manager indicating receipt and review of the initial Breach Report Form. If no confirmation is received within 24 hours, the initial Breach Report Form must be sent directly to the LRP.
4.	The Group Manager will review the initial Breach Report and make a recommendation to the LRP for closing out the report when sufficient and reasonable information confirms that a breach has not occurred.
5.	The Group Manager will notify the appropriate LRP(s) and any field staff as appropriate. The Group Manager will also provide the appropriate LRP(s) with the initial breach report via e-

	mail and insure that the other internal LRP is also cc'ed and receives notice of the suspected breach. (The Group Manager must notify and provide the initial breach report to the LRPs within 24 hours after receiving the completed initial Breach Report Form from the DSHS staff member.)
6.	If the appropriate LRP for that Group is not available, the Group Manager will need to send a separate e-mail to the other internal LRP indicating that the appropriate LRP is not available and response will be needed on his/her part.
7.	If the internal LRPs are not available, the Group Manager will notify the Unit Manager or the next level of management available through telephone and e-mail.
8.	The staff member initially submitting the request must receive an e-mail confirmation from the LRP indicating receipt and review of the initial Breach Report Form.

Investigating a Suspected Breach

1.	After the LRP has received the breach report, the LRP will inform the Security Team of the suspected breach.
2.	The Security Team will be responsible for further investigating the incident. (The Security Team may request further information regarding the incident to be submitted.)
3.	The Security Team will review the initial breach report and complete "Section 2: Security Team Closing Report". The investigation should be finished no later than 7 days following the initial incident date.
4.	The final completed report (Sections 1 and 2) will be sent to both internal LRPs via e-mail.
5.	All media calls related to an internal suspected breach must be referred to the CSHS Communications Public Relations Officer according to DSHS Policy AA-5036 (News Media Policy) http://online.dshs.state.tx.us/policy/agency/aa-5036.htm
6.	Any breach of confidentiality will be investigated immediately to assess causes and implement corrective actions. If a breach of confidentiality is related to a federally sponsored program, the LRP will report it promptly to the appropriate federal program contact.

Action Steps Specific to the Type of Breach

1.	Suspected Breach (Non-breach in protocol): a. A suspected breach is reported and the Security Team investigates the suspected breach. b. The Security Team determines that the suspected breach is neither a breach of protocol nor a breach of confidentiality. c. The Security Team will ensure that the Group Manager communicates the findings to the appropriate DSHS staff member. d. The LRP will be responsible for closing out the report.
2.	Breach in Protocol: a. A suspected breach is reported and the Security Team investigates the suspected breach. b. The Security Team determines that the suspected breach is a breach in protocol but not a breach in confidentiality. (In this case the Security Team has determined that no confidential information has been divulged in any manner but a breach in protocol poses a risk to a breach in confidentiality and recommendations will need to be made accordingly.) c. When only a breach in protocol has occurred, the Security Team will need to determine if the breach was negligent or purposeful. d. The Security Team will recommend the necessary actions to be taken based on the type of breach (negligent or purposeful) to the Group Manager. e. Subsequently, it is the responsibility of the Group Manager to monitor the employee and assure that further breaches in protocol do not occur that may ultimately result in a breach of confidentiality. f. The Group Manager will also assure that the employee causing this breach in

	protocol receives emergency training on security and confidentiality. g. Additionally, disciplinary action may need to be taken by the Group Manager especially when repeated breaches in protocol have occurred. If the employee continues to pose a threat to security of confidentiality, the employee's access to HIV/STD Program information will be limited or rescinded until further personnel actions have been determined.
3.	Breach in protocol and confidentiality: a. A suspected breach is reported and the Security Team investigates the suspected breach. b. The Security Team determines that the suspected breach is a breach in protocol and a breach in confidentiality. (In this case the Security Team has determined that confidential information has been divulged and an immediate response is necessary.) c. When the suspected breach is found to be both a breach of protocol and breach of confidentiality, the Security Team will make appropriate recommendations regarding actions that will need to be taken based on whether the breach is determined to be purposeful or due to negligence. d. Regardless of the type of breach (purposeful or negligent), the following recommendations may be required based on the severity of the breach of confidentiality: • The employee's access to physical and electronic resources must be limited or rescinded until an investigation of the incident is complete. Options for handling the situation include: immediately reassigning the employee to a temporary duty station; obtaining permission from the Unit Chief (to whom the employee is assigned) to send the employee home pending investigation of the breach; or calling law enforcement in extreme situations. • At the discretion of the LRP the following entities may be notified: the Communications Office, the Office of General Counsel, the Commissioner of Health, the Associate Commissioner for Disease Control and Prevention, the Director, Prevention and Intervention Section, the Health Promotion Unit Manager and the HIV/STD Epidemiology and Surveillance Unit Manager and other appropriate senior departmental staff, if appropriate. • Implement new or additional processes to address any deficiencies in the HIV/STD program security and confidentiality policies and procedures.

Follow-Up to a Breach and Maintenance of Files

1.	If a breach has occurred, the Group Manager will submit a follow-up report via e-mail to both LRPs on a monthly basis. The follow-up report will detail the corrective steps (Section 3 of Breach Report Form) that have been taken to resolve the problem to prevent the breach from occurring again.
2.	On a monthly basis, the internal LRPs will confirm receipt of the follow-up Breach Report Form and indicate if the response is appropriate. Monthly follow-up reports will be submitted until corrective actions are concluded or deemed sufficient by the internal LRP(s).
3.	The ORP or designee will retain a file of all completed breach response forms in a locking file cabinet. (Breach Report Forms will be maintained separate from the employees personnel file.)
4.	The ORP's designee will enter all information into the Breach Report Database. The Breach Report Database will be password protected and only the ORP, LRP(s) and designee(s) will have access to the database.
5.	The Group Manager will be responsible for periodically running reports based on the Breach Report Database and determine if any patterns in breaches exist that need to be further addressed.

10.0 Revision History

Date	action
07/02/08	Revisions too numerous to list; therefore treated as new policy. Policy previously identified as 020.051

TEXAS Department of State Health Services	*Policy Number*	302.001
	Effective Date	April 9, 1999
	Revision Date	July 2, 2008
Release of HIV/AIDS and STD Data	*Subject Matter Expert*	Surveillance Specialist
	Approval Authority	Branch Manager
	Signed by	Sharon K. Melville, MD, MPH

1.0 Purpose

This policy describes guidelines for the release or publication of data associated with HIV/AIDS and STD surveillance, epidemiologic, public health follow-up, and the Texas HIV Medication Program (THMP). This policy aligns with requirements in the DSHS HIV and STD Program Operating Procedures and Standards (POPS) (http://www.dshs.state.tx.us/hivstd/pops/default.shtm), the Centers for Disease Control and Prevention's (CDC) Program Operations Guidelines for STD Prevention, (http://www.cdc.gov/std/Program/overview/TOC-PGoverview.htm), and the CDC's Technical Guidance for HIV/AIDS Surveillance Programs (Atlanta, GA; 2006) wherever possible and/or appropriate.

2.0 Authority

All information obtained and compiled by DSHS related to a disease report is confidential and may be used or released only as permitted by Health and Safety Code §81.046. Additionally, DSHS is legally bound by federal assurances of confidentiality (Sections 306 and 308(d) of the Public Health Service Act, 42 US Code 242k and 242m(d)) which prohibit disclosure of any information that could be used to directly or indirectly identify patients. This policy has been written in accordance with the Health and Safety Codes §81.046 and §81.103 and the Texas Administrative Codes §97.146 and §98.13 of Title 25.

3.0 Definitions

Aggregate Data - data which are based on combining individual level information; Aggregate data may contain potentially identifying information, particularly if the aggregated data are very detailed or for a small subset of individuals.

Central Office – the HIV/STD Program, Department of State Health Services (DSHS) main office located in Austin, Texas.

Confidential Information – any information which pertains to a patient that is intended to be kept in confidence or kept secret and could result in the identification of the patient should that information be released.

Confidentiality - the ethical principle or legal right that a physician or other health professional or researcher will prevent unauthorized disclosure of any confidential information relating to patients and research participants

De-identified (Pseudo-anonymous) Data - individual record-level data which has been stripped of personal identifiers (e.g., name, address, social security number) but may contain potentially identifying information (e.g., age, sex, race/ethnicity, locality information) that when combined with other information may identify an individual. If the combining of information could identify an individual, these data are considered confidential.

Demographics – refers to selected population characteristics, including race/ethnicity, sex, and age.

External – entities outside of the DSHS Central Office that the HIV/STD Program contracts with or works in association with to conduct public health activities related to HIV/STD surveillance, epidemiology, public health follow-up and the medication program.

Fifty Rule – refers to the acceptable threshold for the release of aggregate HIV/AIDS and STD surveillance, epidemiologic, and public health follow-up data. The underlying population of the statistic released must be a population of greater than fifty people. The underlying population must also be at least twice the number of cases.

Geocode - is a representation format of a geospatial coordinate measurement used to provide a standard representation of an exact geospatial point location at, below, or above the surface of the earth at a specified moment of time.

Geographic Information System (GIS) – is an information system capable of integrating, storing, editing, analyzing, sharing, and displaying geographically-referenced data.

HIV/STD Program – consists of the two branches of the DSHS Prevention and Preparedness Unit: the HIV/STD Comprehensive Services Branch and the HIV/STD Epidemiology and Surveillance Branch.

Institutional Review Board (IRB) - is a group that has been formally designated to approve, monitor, and review biomedical and behavioral research involving humans with the aim to protect the rights and welfare of the subjects.

Local Responsible Party (LRP) – an official who accepts responsibility for implementing and enforcing HIV/STD policies and procedures related to the security and confidentiality of HIV/STD surveillance, epidemiology, public health follow-up and medication program data and information and has the responsibility of reporting and assisting in the investigative breach process.

Personal Identifier - a datum or collection of data which allows the possessor to determine the identity of a single individual with a specified degree of certainty; a personal identifier may permit the identification of an individual within a given database. Bits of data, when taken together, may be used to identify an individual. Personal identifiers may include name, address or place of residence, social security number, telephone number, fax number, and exact date of birth.

Population - a group of people defined by demographic characteristics such as age, race, sex, or location of residence

Potentially Identifying Information – information which, when combined with other information, could potentially identify an individual or individuals. This includes but is not limited to such information as medical record/case numbers and demographic or locality information that describe a small subset of individuals (e.g., block data, zip codes, race/ethnicity data).

Surveillance - the ongoing and systematic collection, analysis, and interpretation of health data in the process of describing and monitoring a health event. This information is used for assessing public health status, triggering public health action, defining public health priorities and evaluating programs.

4.0 Policy

The policy of DSHS is to ensure that HIV/AIDS and STD data are released and/or published while maintaining patient confidentiality. The policy is also to ensure that individual record-level data containing personal identifiers are only released with proper legal authority. HIV/STD Program staff must assess the potential impact of proposed data releases on confidentiality, and staff responsible for the release of HIV/STD data must take steps to prevent the identification of individuals.

5.0 Persons Affected

Person affected are DSHS employees and external entities that have access to HIV/STD surveillance, epidemiologic, public health follow-up and THMP data.

6.0 Responsibilities

The Local Responsible Party (LRP) is responsible for implementing and enforcing these data release guidelines. For the HIV/STD program, the managers of the HIV/STD Epidemiology and Surveillance Branch and the HIV/STD Comprehensive Services Branch are the LRP, each responsible for the proper release of the information originating from that program area. The HIV/STD Epidemiology and Surveillance Branch Manager will be responsible for the proper release of HIV/STD surveillance and epidemiologic data. The HIV/STD Comprehensive Services Branch Manager will be responsible for the proper release of THMP data and information. The LRP are jointly responsible for the proper release of public health follow-up data.

Regional programs and agencies contracting with the Program for surveillance or public health follow up must designate an LRP to oversee the release of HIV/STD data from their program. Regional programs and contractors that handle HIV/STD surveillance, epidemiologic, and public health follow-up data must develop a policy outlining guidelines for the release of local HIV/STD data or they may choose to adopt the HIV/STD Program's policy.

7.0 Data Release Guidelines

7.1 Aggregate Data

7.1.1 Fifty Rule

Aggregated HIV/AIDS and STD surveillance, epidemiologic, and public health follow-up data may be released if the underlying population consists of more than fifty people. Furthermore, the underlying population must be at least twice the number of cases. The size of the underlying population must be verified through the U.S. Census Bureau. Tables consisting of cells that do not satisfy the Fifty Rule are acceptable for release if those cells have been suppressed. Additional cells may also need to be suppressed to prevent the derivation of the suppressed data. Alternatively, data are acceptable for release if pooled to span a longer time period (i.e., 3 or 5 year periods). Another option is to collapse data categories if the data has been stratified by one or more categories, such as sex or age. All data at the zip code level or smaller and data that do not meet the fifty rule must be reviewed and approved for release by the DSHS HIV/STD Epidemiology and Surveillance Branch Manager. When population data are not available, the DSHS HIV/STD Epidemiology and Surveillance Branch Manager should be consulted.

7.1.2 Geographic Data

Data depicted on a map should be consistent with the aforementioned Fifty Rule. Geographic areas with populations that do not satisfy the Fifty Rule must be aggregated with data from one or more other geographic areas, although mapped data points with values of zero are acceptable for release.

The release of data in a map format created with GIS should not be accompanied by the individual layers and corresponding attribute tables used in the production of the map. The map should be released as a stand-alone image of a final product (e.g., JPEG format).

7.1.3 Medication Program Exception
The THMP may release aggregate program utilization and cost data without adherence to the Fifty Rule. Sub-county level data or stratified data must be reviewed and approved by the THMP manager or designee prior to release. All requests for THMP aggregate data will be processed by THMP staff and tracked by the THMP manager.

7.2 De-identified Individual Record-Level Data

The HIV/STD Program rarely releases de-identified individual record-level data. These data are only released for research or public health purposes, and these data shall only be released with a data sharing agreement in place and upon receiving approval from the LRP.

7.2.1 Geocoded Data
Individual record-level data consisting of geocoded address data for release in a map format or data file should not contain the geographic coordinates of addresses. Instead, individual addresses will identify the geographic level (e.g. county, census tract) to which they were geocoded.

7.2.3 Registry Matching
Confidential HIV/STD surveillance, epidemiologic, and public health follow-up data are routinely matched with data in other disease registries (e.g., cancer, tuberculosis) and data systems to improve data quality as a part of routine disease surveillance. HIV/AIDS and STD data may not be released to other programs for matching. Rather, the comparison of disease registries and other program data should be accomplished by the HIV/STD Program staff. The LRP is responsible for ensuring that data sharing agreements are in place when data are shared for matching purposes and are consistent with HIV/STD Program policies pertaining to the release of data.

7.3 Personally Identified Individual Record-Level Data

The HIV/STD Program strongly discourages the release of individual patient records that contain personal identifiers. In very limited circumstances, a patient's personal records may be released to providers, legal entities, and/or directly to the patient. The HIV/STD Program may also disclose individual patient data for public health purposes.

7.3.1 Patient Records
For requests through the HIV/STD Epidemiology and Surveillance Program, providers, patients and/or their lawyers may request only data relating to the patient. HIV/STD public health follow-up data will not be released to patients, providers, or legal entities under any circumstances, as those data contain partner information.

7.3.2 Public Health Purposes
Following routine matching of confidential HIV/STD surveillance, epidemiologic, and public health follow-up data with data in other disease registries, the HIV/STD Program may provide the other program with data on persons who are also diagnosed with an STD, including HIV. The LRP is responsible for ensuring that data sharing agreements are in place when data are shared and are consistent with HIV/STD Program policies pertaining to the release of data and maintaining confidentiality of the data.

7.3.3 THMP
Due to statutory provisions protecting the confidentiality of the manufacturers' drug pricing data (Federal Omnibus Budget Reconciliation Act of 1990 and in Section 340B of the Public Health Services Act, 42 U.S.C. 256B), drug pricing lists are considered restricted and cannot be released. Client records containing personal identifiers may be released to

treating physicians, servicing pharmacies, contractors, the patient, or other programs as necessary for the client to obtain services. THMP routinely shares THMP data with pharmacy benefit manager contractors, Medicare, and Medicaid. The LRP is responsible for ensuring that data sharing agreements or appropriate contracts are in place when THMP data are shared.

8.0 HIV/STD Program Procedures
HIV/STD Epidemiology, Surveillance and Public Health Follow-Up Data

8.1 Responding to Requests for Aggregated Data

Requests for data present an opportunity for direct interaction between the HIV/STD Program and our customers in the public, the media, the legislature, and other public health agencies. DSHS staff handling data requests should extend the most professional, courteous, accurate and rapid service available. The following procedure provides guidance for fulfilling data requests. DSHS recommends that regional and contracting programs create procedures for handling and tracking data requests that are similar.

Customers commonly initiate data requests via telephone or e-mails. An assigned staff member will work with the customer to complete the data request by clearly defining the specifics of the data requested. For requests of data that the HIV/STD Program does not have, program staff should refer the customer to other sources when possible. Key criteria for defining data requests may include:

- Disease(s) or diagnosis
- Reported cases versus diagnosed cases
- Number of cases, rates, or both
- Time period
- Geographic location(s)
- Demographic crosstabs (e.g., age, sex, race, risk group, etc) or restrictions (e.g., living cases, male cases, female cases, etc)
- Date the data request must be completed

Occasionally, the customer may not know how to define the data needed. In such cases, the assigned staff member may help define the request based on the question(s) the customer is trying to answer. For formal Public Information requests, assigned staff members are **not** permitted by state law to inquire about why the request is being made.

The assigned staff member will gather the customer's contact information, including e-mail address or fax number, in order to send the data. In general, assigned staff members should accept and meet the customer's deadline for receiving the data. If the deadline is unusually short, cannot be met, and/or another deadline cannot be negotiated, consult the LRP.

When completing data requests, assigned staff members should save the syntax and output files in a folder for future reference. These files are recorded in the data request tracking log to allow others to use or modify them for future requests. The requested data are most often saved in an electronic file format (e.g., Excel, Word, html, etc) and e-mailed to the customer. All data files should be clearly annotated, including titles and notes to thoroughly describe what the data represent. Additional notes should also be included to describe any special circumstances or limitations of the data, such as why some cells are suppressed.

If the data results are complete and follow the guidelines described in this policy, they may be sent to the customer along with the staff member's contact information.

If the data require further approval from the LRP due to issues with the data results, such as small underlying populations, then the results may only be sent upon approval. Staff must

not send questionable data through e-mail to the LRP for approval. Until it is approved, the data should be treated as confidential information and may not be e-mailed, even internally. Questionable data are to be hand-delivered.

8.2 Data Request Tracking

8.21 HIV/STD Surveillance Data

During and/or immediately following a request for data, the assigned staff member completing the request will document the request in the EpiDiv Request Log. Providing documentation of data requests in a centralized location allows the HIV/STD Program to quantify who its customers are and how they are being served. In addition, by identifying contact names and file information, future requests for repeat or similar data can be fulfilled more efficiently.

The Request Log is located on the public network in S:\Requests\Epidiv New Request Log.xls. Requests are organized by date. Select the appropriate tab for the year and scroll down to the month that the request was completed. Complete as many of the fields as possible.

8.2.2 Handling Requests from Special Customers

Staff should respond to requests from the media by following Policy Number AA-5007 (http://online.dshs.state.tx.us/policy/agency/aa%2D5036.htm).

All DSHS staff who receives a legislative contact should notify the appropriate Branch Manager immediately. Before responding to a legislative request, staff must obtain approval from appropriate Branch Manager prior to release of data. Immediately following the completion of a legislative request, a Legislative Contact Report should be e-mailed. At minimum, this report will be submitted to the assigned staff member's supervisor, the Branch Managers of the HIV/STD Epidemiology and Surveillance Branch and the Comprehensive Services Branch, the Unit Manager of the Epidemiology and Surveillance Unit, the Director of the Prevention and Intervention Section, the Assistant Commissioner for Prevention and Preparedness, the Office of Governmental Relations, and the individual responsible for legislative liaison at the Division of Prevention and Preparedness.

This report should contain the following information:

- Who made the request – which Legislator's office, contact person's name, telephone number and other contact information
- When the request was received
- What the question or issue was that prompted the request
- Summary of the response or copy of data released
- Any future follow-up required
- Name and contact information for the employee that responded to the request

Staff who receive an Open Records or Public Information Act request should follow Policy Number AA-5007 (http://online.dshs.state.tx.us/policy/agency/aa%2D5007.htm).

8.3 De-identified Data Requests

De-identified individual record-level data are only released upon approval by the LRP. Customers commonly initiate data requests via telephone or e-mail. For HIV/STD surveillance, epidemiologic, and public health follow-up data requests, customers must sign Data Release and Confidentiality Agreements prior to receipt of data. The Data Release and Confidentiality Agreements will specify:

- the permitted uses, disclosures, and final disposition of the data
- who is permitted to use or receive the data

- that the data recipient will use appropriate safeguards to prevent use or disclosure of the information outside that specified by the Data Release and Confidentiality Agreements

The dataset will be prepared by assigned staff and provided to the customer via secured means upon approval by the LRP. The LRP or designee will file the paperwork associated with the request and enter the request in the Data Release Tracking Log. The LRP or designee will provide the customer with a signed copy of the Data Release Agreement and must store hard copies of the agreement. Follow-up will be conducted with customers who receive individual record-level data to ensure that the data and any additional data files created have been properly destroyed on their stated project completion date.

All THMP data requests will be processed by THMP staff and tracked by the THMP manager.

External sites should develop and use their own data release agreement for local individual record-level requests, or the external sites may choose to use the DSHS Data Release Agreement.

Handling Requests for Research Purposes

Requests for individual record-level data from the HIV/STD Epidemiology and Surveillance Branch for research purposes must be reviewed and approved by the DSHS Institutional Review Board (IRB) and the Local Responsible Party. Procedures for submitting data requests to the DSHS IRB can be found at *http://www.dshs.state.tx.us/irb/default.shtm*. The requestor must also obtain approval from an IRB at the institution responsible for oversight of the research program. Prior to releasing datasets, all personal identifiers must be removed. Datasets that contain potentially identifying information must be maintained by the recipient in a manner consistent with the most current DSHS confidentiality and security guidelines regarding physical and electronic security. The staff of the research institution must comply with all security and confidential training requirements.

Upon approval by the IRBs, Data Release and Confidentiality Agreements must be signed prior to releasing the data (See Appendix A). The Data Release Agreement must specify the length of time that the research institution will maintain the data. All the data must be removed from all electronic files and hard copies at the conclusion of the timeframe specified in the Data Release Agreement. The research institution must provide documentation that these data have been destroyed in a confidential manner.
Requests for THMP individual record-level data for research purposes must be reviewed by the DSHS IRB.

8.4 Personally Identified Individual Record-Level Data

8.4.1 Requests From Legal Entities

Requests for individual HIV/STD surveillance, epidemiologic, or THMP patient records initiated via court orders, subpoenas, or legal counsel for a patient must be directed to the DSHS Office of General Counsel. Patients and/or their lawyers must sign a medical record release form before any data are released. The LRP must see the medical record release form and approve before data is released.

8.4.2 Requests by Patients or Providers

Providers requesting patient records or patients requesting their own records through the HIV/STD Epidemiology and Surveillance Branch must be directed to the DSHS Office of General Counsel. A medical record release form must be signed by the patients and the LRP must see the medical release form and approve before data is released. Requests for THMP client records do not need to be directed to the DSHS Office of General Counsel.

9.0 Revision History

Date	Action	Section
07/02/08	Extensive revision too numerous to list, therefore treated as new policy. Previously, this policy was numbered as 020.061	NA

HIV/STD Epidemiology and Surveillance Confidential Information Security Procedures	*Policy Number*	323.001
	Effective Date	July 3, 2008
	Revision Date	July 3, 2008
	Subject Matter Expert	Internal Workgroup
	Approval Authority	Branch Manager
	Signed by	Sharon K. Melville, MD, MPH

1.0 Purpose

This document establishes the general procedures that all HIV/STD surveillance and epidemiologic program staff, located in the Central Office and external sites, are required to follow concerning the collection, transmission, storage and maintenance of confidential information both in the office and in the field.

2.0 Definitions

Advanced Encryption Standard

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data.

Authorized User

Those individuals employed by the program who, in order to carry out their assigned duties have been granted access to confidential information.

Central Office

The HIV/STD Program, Department of State Health Services (DSHS) main office located in Austin Texas.

Confidential information

Any information which pertains to a patient that is intended to be kept in confidence or kept secret and could result in the identification of the patient should that information be released

Confidentiality

The ethical principle or legal right that a physician or other health professional or researcher will prevent unauthorized disclosure of any confidential information relating to patients and research participants

Encryption

The manipulation or encoding of information so that only parties intended to view the information can do so. There are many ways to encrypt information; most commonly available systems involve public key and symmetric key cryptography.

- A public key system uses a mathematically paired set of keys, a public key and a private key. Information encrypted with a public key can only be decrypted with the corresponding private key, and vice versa. Therefore, you can safely publish the public key, allowing anyone to encrypt a message that can be read only by the holder of the private key. Presuming that the private key is known to only one authorized individual, the message is then accessible only to that one individual.
- A symmetric key system is based on a single private key that is shared between parties. Symmetric systems require that keys be transmitted and held securely in order to be

effective, but are considered to be highly effective when the procedures are good and the number of individuals who possess the key is small. In general, the larger the key the more robust the protection.

Global Positioning Device (GPS)
A GPS is typically a hand-held or vehicle-mounted navigational system. It uses Global Positioning System (hence GPS) technology to triangulate any given position using three satellite signals relating to the unit.

Key-Card
A badge containing magnetically coded information, that when placed in the proximity of a reading device unlocks a door. Key cards are used as part of physical security systems.

Local Responsible Party (LRP)
An official who accepts responsibility for implementing and enforcing HIV/STD polices and procedures related to the security and confidentiality of HIV/STD surveillance, epidemiology, public health follow-up and medication program data and information. The LRP has the responsibility of reporting and assisting in the investigative breach process. A Local Responsible Party will be designated both internally and externally. Internally the HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch managers will be designated as the LRP.

Overall Responsible Party (ORP)
The official who accepts overall statewide responsibility for implementing and enforcing these security standards as they apply to HIV/AIDS surveillance data and who may be liable for breach of confidentiality. The state's security policy must indicate the ORP by name.

Password Protected
Files and directories that are protected from unauthorized access by requiring users to enter a password before access is allowed.

Personal Digital Assistants (PDA)
A PDA is a handheld computer, which has many uses, including, but not limited to: calculation, accessing the internet, sending and receiving e-mails, video recording, word processing, and Global Positioning (GPS).

Personal Identifier
A datum or collection of data which allows the possessor to determine the identity of a single individual with a specified degree of certainty; a personal identifier may permit the identification of an individual within a given database. Bits of data, when taken together, may be used to identify an individual. Personal identifiers may include name, address or place of residence, social security number, telephone number, fax number, and exact date of birth.

Removable Storage Device
A device that allows for the transportation of electronic information; there are many types of Removable Storage Devices including, but not limited to: USB port flash drives (memory sticks), diskettes, CD-ROMS, zip disks, tapes, smart cards, and removable hard drives.

External
Entities outside of the DSHS Central Office that the HIV/STD program contracts with or works in association with to conduct public health activities related to HIV/STD surveillance, epidemiology, public health follow-up and the medication program.

Secured Area
A confined physical space where HIV/STD data and information are located with entry limited to staff with authorized access; the secured area is usually defined by hard, floor-to-ceiling walls with a locking door and may include additional measures (e.g., alarms, security personnel).

Security
The protection of surveillance data and information systems, for the purposes of (1) preventing unauthorized release of identifying surveillance information or data from the systems (e.g., preventing a breach of confidentiality) and (2) protecting the integrity of the data by preventing accidental data loss or damage to the systems. Security includes measures to detect, document, and counter threats to the confidentiality or integrity of the systems.

Secure Voicemail
A Voice Mailbox system that is password protected and in which messages are stored on a protected network.

Surveillance
The ongoing and systematic collection, analysis and interpretation of health data in the process of describing and monitoring a health event; this information is used for assessing public health status, triggering public health action, defining public health priorities and evaluating programs.

Wi-Fi (Wireless Fidelity)
Refers to wireless network components that are based on one of the Wi-Fi Alliance's 802.11 standards. The Wi-Fi Alliance created the 802.11 standard so that manufacturers can make wireless products that work with other manufacturers' equipment. This equipment uses high-frequency radio waves rather than wires to communicate. Wi-Fi is commonly used to wirelessly access the Internet or a local network.

Wiki
A piece of server software that allows users to freely create and edit Web page content using any Web browser; Wiki supports hyperlinks and has simple text syntax for creating new pages and cross links between internal pages.

3.0 Physical Security

3.1 Buildings/Offices

- All surveillance and epidemiological confidential information, electronic and paper, must be maintained in a secure locked area with limited access. A secure area is an area which is protected by at least one level of physical security, although it is preferable that HIV information be maintained behind two levels of physical security. A security guard should not be the only level of security. Examples of physical security levels are:
    - Secured access card
    - Locked door
    - Reader code access
- The Local Responsible Party (LRP) for each site is responsible for approving the physical security levels of the site.
- The LRP for each site is responsible for maintaining a **log** which identifies all individuals with access to secured areas.

- Rooms containing confidential information must not have windows which could allow easy entry into the room.
- Keys, key-cards, and codes enabling access to secure areas as defined above must not be shared or loaned.
- Any secured area that allows access to visitors must have a process for tracking visitors' access.
- Visitors to secured areas must be escorted at all times.
- Persons with authorized access to secure areas must be able to identify visitors (e.g. Identification badge).
- Secured doors should not be propped open or disabled unless prior approval to do so has been obtained from the LRP.

3.2 Computer Workstations

- All computer workstations with access to confidential information must be in a secure area. A secure area is one in which there is at least one level of physical security, although it is preferable that computer workstations with access to HIV information be maintained behind two levels of physical security.
- Computer screens must not be readily observable by non-authorized users as they pass through the office area, sit at desks, or approach reception areas. Security screens may be installed on computer monitors to prevent viewing of information on the computer screen by anyone other than the operator.
- Computers used to access confidential information must be password protected at the Windows login level, and have a password protected screensaver program installed and activated.
- All network/computer passwords are to be at least eight characters in length and must be a combination of letters, characters and numbers, and not easily guessed.
- Network/computer passwords must expire based on current password guidelines.
- New or temporary passwords issued to a staff member must be changed upon receipt of the password.
- Computer passwords must not be shared with others.
- No one should access a computer or network using another person's access without written authorization.
- If a password's security is in doubt, it must be changed immediately.
- Passwords should not be written down but when necessary to do so, the stored passwords must be encrypted.
- Computer workstations must be locked (Ctrl/Alt/Delete - Lock Workstation) when a workstation is left unattended.
- Internet Control Message Protocol (ICMP) should not allow "Redirect Services" to devices (i.e. Blackberries) not authorized by the specific network administrators.
- Services running on the specific network should not allow "remote desktop" by individuals (i.e. computers) not in the network.
- Local hosting of servers (i.e. "wikis") on computers that contain confidential information is a security risk.
- Confidential data must not be accessed or worked with on any computer that is not secure.

4.0 Handling Paper Records

- When not in use, all documents with surveillance and epidemiological confidential information must be stored in a locked file cabinet in a locked secure area.
- Documents with confidential information should be returned to their secured storage after their use has been completed.
- Documents with confidential information must not be readily observable by non-authorized users as they pass through the office, sit at desks, or approach reception areas.
- When documents with confidential information are taken from a secured area they must be transported in a secure container (e.g. locked briefcase), not visible in a car, and must contain the minimum amount of confidential information necessary to do business and, where possible, must be coded to disguise any information that could easily be associated with HIV or AIDS and/or identity of the individual.
- Confidential information will be maintained and destroyed according to the DSHS records retention policy for surveillance and epidemiologic information or the local records retention policy.
- Documents with confidential information must be shredded using a shredder that is of commercial quality and has a crosscutting feature before disposing of them.
- Shredding of documents containing confidential information must be conducted by persons authorized to view the confidential information.
- Documents containing confidential information that are waiting to be shredded must be stored in a secure area.
- Stored documents with confidential information must be clearly marked as containing confidential information.
- Working with confidential surveillance and epidemiologic information at home (telecommuting) is prohibited.
- Confidential information will not routinely be taken to a private residence but if unavoidable then specific approval must be obtained from their supervisor or the LRP.
- Prior approval must be obtained from their supervisor or the LRP when business travel precludes the return of confidential surveillance information to the secured area by the close of business on the same day.

5.0 Telephone/Faxing/E-mail

5.1 Telephone (including cell phones)

- Telephone calls concerning confidential information must be made in an area where conversations cannot be **overheard**.
- Personnel must reasonably ascertain that phone contacts are legitimate before discussing confidential information on the phone.
- On the telephone, personnel will only share the minimum amount of confidential information needed to accomplish the surveillance or epidemiological objective of the call.
- Confidential information must never be left on voicemail systems unless they are secure systems (cell phone voice mail systems are generally not secure) or there is authorization from the call recipient to leave confidential information.
- Outgoing voicemail messages on telephones with non-secure voicemail, must ask the caller to leave only their name and number.
- Outgoing voicemail messages on telephones must not identify staff as being employed by the HIV/STD program.

- If a person is on a confidential call and they can hear other conversations over the line (often called cross talk) or experience similar issues, the conversation must end immediately and be reported to the LRP.

5.2 Faxing

- Facsimile transmission of confidential information must only be done when other methods of sending information are unavailable or would delay the timely provision of services.
- Confidential information sent using a facsimile must be faxed under a cover sheet. The cover sheet must not contain the words HIV, AIDS, or STD anywhere on it.
- The HIV/AIDS Reporting System (HARS) cityno and stateno are to be considered as identifying variables and should not be included on faxes.

- The information to be faxed must be
    - de-identified (client's name and all other identifying information removed) OR
    - the identifying information must be sent in a separate fax transmission only after the sender has confirmed receipt of the first fax with the receiver; OR
    - All HIV/STD related information has been removed or converted to a code
- Anyone sending a fax must confirm that the information faxed was received by the intended recipient
- Fax machines used to send or receive confidential information must be located in a secure area.
- Programs are encouraged to use separate fax machines instead of multifunctional machines which include faxing capabilities.

5.3 E-Mail

- E-mail transmissions, encrypted or non-encrypted, containing any confidential information must not be sent. The use of email attachments for the purpose of transmitting confidential information is prohibited (see Section V: Electronic Data Handling for methods of transmitting electronic data).
- The HARS cityno and stateno are to be considered as identifying variables and should not be included on emails or email attachments.
- Email and confidential information must not be accessed simultaneously to avoid accidental submission of data through this system. This includes any electronic device with internet capabilities.

6.0 Handling Confidential Mail

6.1 Incoming Mail

- All mail marked “confidential” must be checked by authorized personnel only and kept in a secured location until it is processed.
- Mail marked “confidential” should only be opened by the addressee.
- The person in charge of receiving the confidential mail must record the receipt of all mail into a log book, by the end of each day. Each log entry must note the name of the sender, what was received, and the date of receipt.
- The person in charge of receiving the confidential mail must contact the sender on the day of receipt to notify them that their mail was received.

6.2 Outgoing Mail

- All confidential HIV information sent using the mail system must be double enveloped. Confidential HIV information must first be first placed in a sealed, taped non-addressed envelope marked “CONFIDENTIAL”; that envelope is then placed in a second sealed and taped envelope marked “CONFIDENTIAL” and “TO BE OPENED BY ADDRESSEE ONLY.”
- All confidential STD (non-HIV) information sent using the mail system must be placed in a sealed, taped envelope that is marked “CONFIDENTIAL and “TO BE OPENED BY ADDRESSEE ONLY.” The envelope must contain the return address of the sender.
- The outer envelope must contain the return address of the sender. The words HIV/AIDS/STD must not appear in the body of the address or return address. This includes address stamps and/or pre-addressed envelopes.

7.0 Handling Electronic Data

7.1 Electronic Data Access

- Network drives, which contain confidential information, must have controls in place that enable only authorized users access.
- Staff **may not** attempt to access any data, program, or system for which they do not have approved authorization.

7.2 Electronic Data Storage

- Electronic data must be held in a technologically secure environment; the number of data repositories and the number of permitted users must be kept to a minimum.
- At the Central Office, all electronic confidential information must be stored on a secure password protected network drive on a “private computer.” A “private computer” is a computer which is not connected to the Internet, but is part of a DSHS network. The password for the secure drives, which contain confidential information, will only be given to authorized users.
- At external sites, all confidential information must either be stored on a computer which is not connected to a network (i.e. stand alone computer) or on a secure drive of a secure network (e.g. network with restricted access and/or firewall protection).
- No data is to be stored on the hard drive of any computer connected to a local or wide area network (WAN).
- When storing datasets, which are no longer in use, the dataset must be encrypted using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf) and stored either on a stand alone computer or on a secure drive.

7.3 Electronic Data Transmission

- Confidential electronic information being transferred between the Central Office and external sites, and between external sites, must be encrypted and transferred using secure networks approved by the LRP.
- Confidential information transmitted electronically between Central Office and external sites and between external sites, must be sent over the Health Alert Network (HAN)/Public Health Information Network (PHIN) as follows:
  1. Encrypt data on a secure drive using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197 and password protected. The password for the file must only be

shared with the recipient of the data and sent separately from the data. WinZip 9.0 or later can be used to encrypt the file.

2. Once the data has been encrypted, transfer the encrypted data from the secure drive to a location with access to the Health Alert Network.
3. Log in to the HAN/PHIN and upload your data.
4. Send an email to the person who will be receiving the file to inform them that the file has been uploaded; give them the encryption password.

- All confidential electronic data received by the Central Office from an external agency (e.g. electronic lab reports) will follow the same standards as those listed above.
- Surveillance and epidemiologic data must have personal identifiers removed (an analysis dataset) if taken out of the secured areas or accessed from an unsecured area.

8.0 Removable, External Storage Devices and Laptops

All staff that is authorized to access confidential information must be individually responsible for protecting their assigned/own laptop or other portable devices including, but not limited to: PDA, blackberries, cell phones, flash drives, diskettes, CD-ROMS, zip disks, tape backups, removable hard drives, smart cards, and/or GPS systems.

8.1 Laptops

- Confidential information **may not** be stored on the hard drive of a laptop computer. All confidential information must be encrypted, using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197, and stored on a removable storage device. The removable storage device containing the data must be separated from the laptop and stored in a secure location when not in use.
- When working with confidential information on a laptop computer, staff must ensure that unauthorized users cannot view the computer screen.
- Laptops used as a work computer fall under the same confidentiality and security guidelines as workstations (see physical security section).
- Laptops shall not be left unattended in non-secure areas. If you must leave a laptop in a room, the room must be locked or the laptop and other confidential information must be placed in a locked file cabinet.
- When traveling with a laptop, use a lockable carrying case for the laptop. If you do not have a lockable carrying case, a form-fitting padded sleeve for the laptop carried in a backpack, courier bag, briefcase, or other common nondescript carrying case may be used if approved by the LRP.
- When transporting a laptop, it is safer to rent or use a car with a locking trunk (not a hatchback/minivan/SUV). Regardless of vehicle type, laptops must never be visible from outside of the car.
- The laptop must always be locked up or stored in a locked file cabinet when it is not being used.
- Laptop and notebook computers with wireless connectivity capabilities (built-in or attached) must be disabled while working with confidential information.

8.2 Removable Storage Devices

- All confidential information placed on a removable storage device must be encrypted, using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197, and password protected. The password must be stored separately from the device.

- Any removable storage device containing confidential information is to be stored following the physical and electronic standards of this document.
- Removable storage devices containing confidential information must not be taken to a private residence unless specific permission has been granted by the LRP.
- Removable storage devices no longer in use must be destroyed.
- Acceptable methods of sanitizing diskettes and other storage devices that previously contained sensitive data include overwriting or degaussing (demagnetizing) before reuse. Alternatively, the diskettes and other storage devices may be physically destroyed (e.g., by incineration, shredding). Such physical destruction would include the device, not just the plastic case around the device.

8.3 Personal Storage Devices (PDA)/Blackberries/Cell Phones

- Security for PDA, blackberries, cell phone or any equivalent system will follow all electronic media and physical storage standards listed in this document.
- No confidential information will be stored on, or accessed from, a PDA, blackberry, cell phone or any equivalent system.
- PDA, blackberries, cell phone or any equivalent systems must be turned off when not in use.
- Functions of the PDA, blackberries, cell phone or any equivalent systems that are not immediately employed in the use of the system, (e.g. “Roaming”, “Text Messaging”, “Bluetooth”, photo capabilities) must be disabled.

9.0 Revision History

Date	Action	Section
07/03/08	This is a new procedure	

HIV/STD Public Health Follow-Up (PHFU) Confidential Information Security Procedures	*Policy Number*	322.001
	Effective Date	July 3, 2008
	Revision Date	July 3, 2008
	Subject Matter Expert	Internal Workgroup
	Approval Authority	Branch Manager
	Signed by Sharon K. Melville, MD, MPH	

1.0 Purpose

This document establishes the general procedures that all HIV/STD field and support staff, located in the DSHS regional and contract sites are required to follow concerning the collection, transmission, storage and maintenance of confidential information. See the HIV and STD Program Operating Procedures and Standards (POPS) (http://www.dshs.state.tx.us/hivstd/pops/default.shtm) for more information about PHFU associated with HIV-positive test results and general follow up practices and procedures.

2.0 Responsibilities

Disease Intervention Specialists (DIS) will not divulge the specific nature of his/her professional capacity to unauthorized persons in the course of disease intervention activities. Information gained in the course of work activity will not be divulged to unauthorized persons in any manner that may be construed to link an individual with a communicable disease. The DIS will handle each situation in a professional manner that safeguards the privacy of individuals.

3.0 Definitions

Advanced Encryption Standard

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data.

Authorized User

Those individuals employed by the program who, in order to carry out their assigned duties have been granted access to confidential information.

Central Office

The HIV/STD Program, Department of State Health Services (DSHS) main office located in Austin Texas.

Confidential Information

Any information which pertains to a patient that is intended to be kept in confidence or kept secret and could result in the identification of the patient should that information be released.

Confidentiality

The ethical principle or legal right that a physician or other health professional or researcher will prevent unauthorized disclosure of any confidential information relating to patients, and research participants

Encryption
The manipulation or encoding of information so that only parties intended to view the information can do so. There are many ways to encrypt information; most commonly available systems involve public key and symmetric key cryptography.

- A public key system uses a mathematically paired set of keys, a public key and a private key. Information encrypted with a public key can only be decrypted with the corresponding private key, and vice versa. Therefore, you can safely publish the public key, allowing anyone to encrypt a message that can be read only by the holder of the private key. Presuming that the private key is known to only one authorized individual, the message is then accessible only to that one individual.
- A symmetric key system is based on a single private key that is shared between parties. Symmetric systems require that keys be transmitted and held securely in order to be effective, but are considered to be highly effective when the procedures are good and the number of individuals who possess the key is small. In general, the larger the key the more robust the protection.

Global Positioning Device (GPS)
A GPS is typically a hand-held or vehicle-mounted navigational system. It uses Global Positioning System (hence GPS) technology to triangulate any given position using three satellite signals relating to the unit.

Key-Card
A badge containing magnetically coded information, when placed in the proximity of a reading device unlocks a door. Key cards are used as part of physical security systems.

Local Responsible Party (LRP)
An official who accepts responsibility for implementing and enforcing HIV/STD polices and procedures related to the security and confidentiality of HIV/STD surveillance, epidemiology, public health follow-up and medication program data and information. The LRP has the responsibility of reporting and assisting in the investigative breach process. An LRP will be designated both internally and externally. Internally the HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch managers will be designated as the LRP.

Password Protected
Files and directories that are protected from unauthorized access by requiring users to enter a password before access is allowed.

Personal Digital Assistants (PDA)
A PDA is a handheld computer, with many uses, including, but not limited to: calculation, accessing the internet, sending and receiving e-mails, video recording, word processing, and Global Positioning (GPS).

Personal Identifier
A datum or collection of data which allows the possessor to determine the identity of a single individual with a specified degree of certainty; a personal identifier may permit the identification of an individual within a given database. Bits of data, when taken together, may be used to identify an individual. Personal identifiers may include name, address or place of residence, social security number, telephone number, fax number, and exact date of birth.

Removable Storage Device
A device that allows for the transportation of electronic information; there are many types including, but not limited to: USB port flash drives (memory sticks), diskettes, CD-ROMS, zip disks, tapes, smart cards, and removable hard drives.

External
Entities outside of the DSHS Central Office that the HIV/STD program contracts with or works in association with to conduct public health activities related to HIV/STD surveillance, epidemiology, public health follow-up and the medication program.

Secured area
A confined physical space where HIV/STD data and information are located with entry limited to staff with authorized access; the secured area is usually defined by hard, floor-to-ceiling walls with a locking door and may include additional measures (e.g., alarms, security personnel).

Security
The protection of surveillance data and information systems, for the purposes of (1) preventing unauthorized release of identifying surveillance information or data from the systems (e.g., preventing a breach of confidentiality) and (2) protecting the integrity of the data by preventing accidental data loss or damage to the systems. Security includes measures to detect, document, and counter threats to the confidentiality or integrity of the systems.

Secure Voicemail
A Voice Mailbox system that is password protected and in which messages are stored on a protected network.

Surveillance
The ongoing and systematic collection, analysis and interpretation of health data in the process of describing and monitoring a health event; this information is used for assessing public health status, triggering public health action, defining public health priorities and evaluating programs.

Wi-Fi (Wireless Fidelity)
Refers to wireless network components that are based on one of the Wi-Fi Alliance's 802.11 standards. The Wi-Fi Alliance created the 802.11 standard so that manufacturers can make wireless products that work with other manufacturers' equipment. This equipment uses high-frequency radio waves rather than wires to communicate. Wi-Fi is commonly used to wirelessly access the Internet or a local network.

Wiki
A piece of server software that allows users to freely create and edit Web page content using any Web browser; Wiki supports hyperlinks and has simple text syntax for creating new pages and crosslink between internal pages.

4.0 Physical Security

4.1 Buildings/Offices

- All confidential information, electronic and paper, must be maintained in a secure area. A secure area is an area which is protected by at least one level of physical security, although it is preferable that HIV/STD information be maintained behind two levels of physical security. Examples of physical security levels are:
    - Secured access card reader access
    - Locked door
    - Security guard
- The Local Responsible Party (LRP) for each site is responsible for approving the physical security levels of the site.
- The LRP for each site is responsible for maintaining a **log** that identifies all individuals with access to secured areas.
- Rooms containing confidential information should not have windows that could allow easy entry into the room.
- Keys, key-cards and codes enabling access to secured facilities must not be shared or loaned.
- Any secured area that allows access to visitors must have a process for tracking visitors' access.
- Visitors to secured areas must be escorted at all times.
- Persons with authorized access to secure areas must be able to identify visitors (e.g. DSHS or local badge).
- Secured doors should not be propped open or disabled unless prior approval of the LRP has been obtained.

4.2 Computer Workstations

- All computer workstations with access to confidential information must be in a secure area. A secure area is one in which there is at least one level of physical security, although it is preferable that computer workstations with access to HIV/STD information be maintained behind two levels of physical security.
- Computer screens must not be readily observable by non-authorized users as they pass through the office area, sit at desks or approach reception areas.
- Computers used to access to confidential information must be password protected at the Windows login level.
- All network/computer passwords are to be at least eight characters in length and must be a combination of letters, characters and numbers, and not easily guessed.
- Network/computer passwords must expire based on current password guidelines.
- New or temporary passwords issued to a staff member must be changed upon receipt of the password.
- Computer passwords must not be shared with others.
- No one should access a computer or network using another person's access without written authorization.
- If a password's security is in doubt, it must be changed immediately.
- Stored passwords must be encrypted.
- Computer workstations must be locked (Ctrl/Alt/Delete - Lock Workstation) when a workstation is left unattended.

- Internet Control Message Protocol (ICMP) should not allow “Redirect Services” to devices (i.e. Blackberries) not authorized by the specific network administrators.
- Services running on the specific Network should not allow "remote desktop" by individuals (i.e. computers) not in the network.
- Local hosting of servers (i.e. “wikis”) on computers that contain confidential information is a security risk.
- Confidential data must not be accessed or worked with on any computer that is not secure.

5.0 Handling Paper Records

5.1 In the Office

- When not in use, all documents with confidential information must be stored in a locked file or locked room in a secure area.
- Documents with confidential information must not be readily observable by non-authorized users as they pass through the office, sit at desks or approach reception areas.
- When documents with confidential information are taken from a secured area within the work space they must contain the minimum amount of confidential information necessary to do business and, where possible, must be coded to disguise any information that could easily be associated with HIV/STD and/or identity of the individual.
- Documents with confidential information should be returned to their secured storage immediately after their use has been completed.
- Confidential information will be maintained and destroyed according to the DSHS records retention policy for field record information or the local records retention policy.
- Documents with confidential information must be shredded using a shredder that is of commercial quality and has a crosscutting feature before disposing of them.
- Stored documents with confidential information must be clearly marked as containing confidential information.
- Confidential documents to be shredded, must either be under the direct control of the staff member, or placed in a designated container labeled “confidential material to be shredded” in a secure area.
- Copies of a Field Record will not be made for any unauthorized purpose.
- Removing Interview Records from the workplace is prohibited.
- The existence or contents of the Interview Record will not be divulged to any unauthorized persons.
- Completed copies of the Interview Record will not be destroyed except as directed by the supervisor and in the manner described for the Field Record.

5.2 Outside the Office

- Workers should take only confidential information that will be immediately used from a secured area.
- Confidential information will not be left unattended in any place or area to which unauthorized persons may reasonably gain access. If a Field Record is lost, the matter is reported to the supervisor immediately.

- Confidential information (field records) will not be taken to a private residence, place of business, or any other location outside a DIS' vehicle other than their own home.
- When documents with confidential information (e.g., field records, test results to be provided to a client) are taken from a secured area to the field they must contain the minimum amount of confidential information necessary to do business and, where possible, must be coded to disguise any information that could easily be associated with HIV/STD.
- The contents of the Field Record will not be divulged to any unauthorized persons. If investigative records are taken into the field, they will be carried in a way to insure against being lost or displayed in any way. The Field Records will be properly coded and code sheets will not be kept in the pouch

6.0 Telephone/Faxing/Email

6.1 Telephone (including cell phones)

- Telephone calls concerning confidential information must be made in an area where conversations cannot be **overheard**.
- Personnel must reasonably ascertain that phone contacts are legitimate before discussing confidential information on the phone.
- On the telephone, personnel will only share the minimum amount of information to accomplish PHFU
- The sharing of specific information about individuals with an authorized person will be done according to local policies and only after taking reasonable precautions to confirm the identity of the authorized person.
- Laboratory test results may be furnished to clients over the telephone in accordance with local policies and safeguards. This includes notifying clients of a negative HIV test result. HIV positive results will not be divulged by telephone.
- Confidential information must never be left on voicemail systems unless they are secure systems or there is authorization (verbal or written) from the call recipient to leave confidential information.
- Outgoing voicemail messages on telephones with non-secure voicemail, must ask the caller to only leave their name and number.
- Outgoing voicemail messages on telephones must not identify staff as being employed by the HIV/STD program.
- If a person is on a confidential call and they can hear other conversations over the line (often called cross talk) or experience similar issues, the conversation must be ended immediately and reported to the LRP.

6.2 Faxing

- Facsimile transmission of confidential information must only be done when other methods of sending information are unavailable or would delay the timely provision of services.
- Confidential information sent using a facsimile must be faxed under a cover sheet. The cover sheet must not contain the words HIV, AIDS, or STD anywhere on it.

- The information to be faxed must be:
    - de-identified (client's name and all other identifying information removed) OR
    - the identifying information must be sent in a separate fax transmission only after the sender has confirmed receipt of the first fax with the receiver; OR
    - All HIV/STD related information has been removed or converted to a code
- Senders of faxes will confirm that the information faxed was received by the intended recipient
- Fax machines used to send or receive confidential information must be located in a secure area.
- Programs are encouraged to use separate fax machines instead of multifunctional machines which include faxing capabilities.

6.3 Email

- E-mail transmissions, encrypted or non-encrypted, containing any confidential information must not be sent. The use of email attachments for the purpose of transmitting confidential information is prohibited (see Section V: Electronic Data Handling for methods of transmitting electronic data). Note: this does not include emails sent using the **Internet Contact Policy** set forth in Attachment 'A' of Chapter 6 of the POPS since no confidential information is contained in the e-mail. http://www.dshs.state.tx.us/hivstd/pops/POPS.doc#chapter6
- Emails following the Internet Contact Policy may be sent by HIV/STD program staff as part of PHFU. This also encompasses PHFU through chat room contact. The procedures for accomplishing this in a confidential manner are set forth in the above-mentioned attachment.
- Email and confidential information must not be accessed simultaneously to avoid accidental submission of data through this system. This includes any electronic device with internet capabilities.

7.0 Handling Confidential Mail.

- All HIV/STD referrals sent using the mail system must be placed in a sealed envelope that is marked "CONFIDENTIAL."
- The envelope must contain the return address of the sender. The words HIV/AIDS/STD must not appear in the body of the address or return address. This includes any address stamps and/or pre-addressed envelopes.

8.0 Handling Electronic Data

8.1 Electronic Data Access

- Network drives that contain confidential information must have controls in place that only enable only authorized users' access.
- Staff **may not** attempt to access any data, program, or system for which they do not have approved authorization.

8.2 Electronic Data Storage

- Electronic data must be held in a technologically secure environment; the number of data repositories and the number of permitted users must be kept to a minimum.
- At the Central Office, all electronic confidential information must be stored on a secure password protected network drive on a "private computer." A "private computer" is a computer that is not connected to the Internet, but is part of a DSHS network. The password for the secure drives, which contain confidential information, will only be given to authorized users.
- At external sites, all confidential information must either be stored on a computer that is not connected to a network (i.e. stand alone computer) or on a secure drive of a secure network (e.g. network with restricted access and/or firewall protection).
- No confidential data are to be stored on the hard drive of any computer connected to a local or wide area network.
- When storing datasets that are no longer *in use, the dataset must be encrypted using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf) and stored either on a stand alone computer or on a secure drive.*

8.3 Electronic Data Transmission

- Confidential electronic information being transferred between the Central Office and external sites, and between external sites, must be encrypted and transferred using secure networks.
- Confidential information transmitted electronically between Central Office and external sites and between external sites, must be sent over the Health Alert Network (HAN)/Public Health Information Network (PHIN) as follows:
    1. Encrypt data on a secure drive using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197 and password protected. The password for the file must only be shared with the recipient of the data and sent separately from the data. WinZip 9.0 or later can be used to encrypt the file.
    2. Once the data has been encrypted, transfer the encrypted data from the secure drive to a location with access to the Health Alert Network.
    3. Log in to the HAN/PHIN and upload your data
    4. Send an email to the person who will be receiving the file to inform them that the file has been uploaded; give them the encryption password

9.0 Removable External Storage Devices and Laptops

All staff that are authorized to access confidential information must be individually responsible for protecting their assigned/own laptop, or other portable devices including, but not limited to: PDA, blackberries, cell phones, flash drives, diskettes, CD-ROMS, zip disks, tape backups, removable hard drives, smart cards, and/or GPS systems.

9.1 Laptops

- Confidential information **may not** be stored on the hard drive of a laptop computer. All confidential information must be encrypted, using encryption

software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197, and stored on a removable storage device. The removable storage device containing the data must be separated from the laptop and stored in a secure location when not in use.

- When working with confidential information on a laptop computer, staff must ensure that no unauthorized users can view the computer screen.
- Laptops used as a work computer fall under the same confidentiality and security guidelines as workstations (see physical security section).
- Laptops shall not be left unattended in non-secure areas. If you must leave a laptop in a room, the room must be locked or the laptop and other confidential information must be placed in a locked file cabinet.
- When traveling with a laptop, use a lockable carrying case for the laptop. If you do not have a lockable carrying case, a form-fitting padded sleeve for the laptop carried in a backpack, courier bag, briefcase, or other common nondescript carrying case may be safer.
- When transporting a laptop, it is safer to rent or use a car with a locking trunk (not a hatchback/minivan/SUV). Regardless of vehicle type, laptops must never be visible from outside of the car.
- The laptop must always be locked up or stored in a locked file cabinet when it is not being used.
- Laptop and notebook computers with wireless connectivity capabilities (built-in or attached) must be disabled while working with confidential information.

9.2 Removable Storage Devices

- All confidential information placed on a removable storage device must be encrypted, using encryption software that meets Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197, and password protected. The password must be stored separately from the device.
- Any removable storage device containing confidential information is to be stored following the physical and electronic standards of this document.
- Removable storage devices containing confidential information must not be taken to a private residence unless specific permission has been granted by the LRP.
- Removable storage devices no longer in use must be destroyed.
- Acceptable methods of sanitizing diskettes and other storage devices that previously contained sensitive data include overwriting or degaussing (demagnetizing) before reuse. Alternatively, the diskettes and other storage devices may be physically destroyed (e.g., by incineration, shredding). Such physical destruction would include the device, not just the plastic case around the device.

9.3 Personal Storage Devices (PDA)/Blackberries/Cell Phones

- Security for PDA, blackberries, cell phone or any equivalent system will follow all electronic media and physical storage standards listed in this document.
- No confidential information will be stored on, or accessed from, a PDA, blackberry, cell phone or any equivalent system.
- Functions of the PDA, blackberries, cell phone or any equivalent systems that are not immediately employed in the use of the system (e.g. “Roaming”, “Text messaging”, “Bluetooth”, photo capabilities) must be disabled.

9.4 GPS systems

- Staff is responsible for ensuring that their GPS systems are secured from damage and/or theft.
- Staff is responsible for ensuring that the address information entered into these systems cannot be linked in any way with the HIV/STD client.

10.0 Revision History

Date	Action	Section
07/03/08	This is a new procedure	

TEXAS Department of State Health Services	*Policy Number*	300.001
	Effective Date	July 2, 2008
	Revision Date	July 2, 2008
	Subject Matter Expert	Special Projects
Overall Responsible Party for HIV/AIDS Surveillance Data	*Approval Authority*	Branch Manager
	Signed by	Sharon K. Melville, MD, MPH

1.0 Purpose
The purpose of this document is to provide for a clear line of responsibility in the area of data security and the maintenance of confidential HIV/AIDS surveillance information.

2.0 Definitions
Overall Responsible Party (ORP) – a public official with sufficient authority to make decisions about statewide HIV/AIDS surveillance operations; the ORP is responsible for the security and confidentiality of the HIV/AIDS surveillance system.

3.0 Background
The Centers for Disease Control and Prevention (CDC) HIV/AIDS Surveillance Cooperative Agreement and the CDC HIV/AIDS Surveillance Security and Confidentiality Guidelines require each grantee to have a policy in place that names the individual who is the ORP.

4.0 Authority
CDC Technical Guidance for HIV/AIDS Surveillance Programs (Atlanta, GA 2006)

5.0 Policy
Sharon K. Melville, MD, MPH, Manager, HIV/STD Epidemiology and Surveillance Branch, Department of State Health Services, is the ORP for the state of Texas.

6.0 Responsibilities
The ORP has responsibility for the security of the surveillance system (including processes, data, information, software, and hardware) and may have liability for any breach of confidentiality. The ORP is responsible for determining how surveillance information will be protected when it is collected, stored, analyzed, released, and dispositioned.

7.0 Procedures
The name of the individual, who is designated as the ORP, rather than an organizational position, must be provided to CDC annually.

8.0 Revision History

Date	Action	Section
April 1, 2008	This is a new policy	n/a

HIV/STD Confidential Information Security Policy	*Policy Number*	301.001
	Effective Date	July 2, 2008
	Revision Date	July 2, 2008
	Subject Matter Expert	Surveillance Specialist
	Approval Authority	Branch Manager
	Signed by	Sharon K. Melville, MD, MPH

1.0 Purpose

The purpose of this policy is to define security standards for protecting the confidential information collected and maintained by the HIV/STD program associated with surveillance, epidemiology, public-health follow-up, and the Texas HIV Medication Program. This policy addresses the administrative, physical, and technical safeguards for the security of confidential information.

This policy has been written in alignment with requirements in the Department of State Health Services (DSHS) *HIV and STD Program Operating Procedures and Standards (POPS)* (http://www.dshs.state.tx.us/hivstd/pops/default.shtm), the DSHS IR-2204 Information Security Policy **(**http://online.dshs.state.tx.us/it/standards/securitystd.htm), Computer Usage Policy IR-2202, the Centers for Disease Control and Prevention's (CDC) Program Operations Guidelines for STD Prevention, (http://www.cdc.gov/std/Program/overview/TOC-PGoverview.htm), and the CDC's *Technical Guidance for HIV/AIDS Surveillance Programs* (Atlanta, GA; 2006), wherever possible and/or appropriate.

2.0 Background

In fulfilling its mission to prevent, treat and control the spread of HIV, STDs and other communicable diseases, the DSHS HIV/STD program, its contractors and external partners obtain personal and private information regarding individuals they serve. The HIV/STD program must be vigilant in maintaining the integrity of the systems that contain this information.

3.0 Authority

V.T.C.A., Penal Code, Chapter 16, Chapter 33; V.T.C.A. Health and Safety Code, 81.046 and 81.103-81.104; V.T.C.A., Texas Government Code, Chapter 552

4.0 Definitions

Central Office: The HIV/STD Program, Department of State Health Services (DSHS) main office located in Austin Texas.

Confidential information: Any information which pertains to a patient that is intended to be kept in confidence or kept secret and could result in the identification of the patient should that information be released.

Confidentiality: The ethical principle or legal right that a physician or other health professional or researcher will prevent unauthorized disclosure of any confidential information relating to patients, and research participants.

Local Responsible Party (LRP): An official who accepts responsibility for implementing and enforcing HIV/STD polices and procedures related to the security and confidentiality of HIV/STD surveillance, epidemiology, public health follow-up and medication program data and information. The LRP also has the responsibility of reporting and assisting in the investigative breach process.

A Local Responsible Party will be designated both internally and externally. Internally the HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch managers will be designated as the Local Responsible Parties.

External: Entities outside of the DSHS Central Office that the HIV/STD program contracts with or works in association with to conduct public health activities related to HIV/STD surveillance, epidemiology, public health follow-up and the medication program.

Security: The protection of surveillance data and information systems for the purposes of (1) preventing unauthorized release of identifying surveillance information or data from the systems (e.g., preventing a breach of confidentiality) and (2) protecting the integrity of the data by preventing accidental data loss or damage to the systems. Security includes measures to detect, document, and counter threats to the confidentiality or integrity of the systems.

5.0 Policy

It is the policy of the DSHS HIV/STD Program that information collected to prevent, treat, and control the spread of HIV and STDs will be protected and maintained to ensure patient confidentiality.

6.0 Persons Affected

This policy applies to all persons who may have access to confidential HIV/STD information associated with surveillance, epidemiology, public health follow up, and the Texas HIV Medication Program. This includes DSHS HIV/STD Program employees (permanent and temporary), IT staff, volunteers, students, and DSHS HIV/STD Program contractors.

7.0 Responsibilities

All persons affected by this policy (specified in section 6.0) are required to follow this policy and the relevant procedures associated with this policy.

- All persons must complete the following before being given access to confidential information:
    - Sign a confidentiality agreement that affirms individual responsibility for keeping client information and data confidential. The original must be stored in the employee's personnel file and a copy must be maintained by the employee. The confidentiality agreement must be signed annually.
    - Sign an assurance that they have reviewed HIV/STD Program security policies and procedures relevant to their position.
    - Successfully complete confidentiality and security training. The date(s) of the training(s) must be documented in the employee's personnel file. For DSHS employees, this training will be in addition to the security awareness and security/computer usage training required by DSHS policy

- All persons are individually responsible for ensuring that the confidential information they work with is protected. This responsibility includes protecting all passwords, keys, and codes that enable access to confidential information.

- All persons are responsible for reporting possible security risks to the LRP.

- All persons are individually responsible for protection of his/her own desk/work area, workstation, laptops or other devices associated with confidential information.

- All persons are responsible for challenging those persons who are not authorized to access confidential information.

- Confidential information gained in the course of work activity will not be divulged to unauthorized persons.

- Upon resignation or termination, all confidential information and keys or devices that enable access to physical and electronic locations where confidential information may be stored must be returned to his/her immediate supervisor.

Local Responsible Party

- All external sites and the Central Office must designate a Local Responsible Party (LRP).
- Internally the HIV/STD Epidemiology and Surveillance and HIV/STD Comprehensive Services Branch managers will be designated as the Local Responsible Parties.
- The LRP will approve any HIV/STD program staff requiring access to confidential information maintained by the HIV/STD Program. The LRP will grant authorization to persons who have a work-related need to view confidential information.
- The LRP will ensure that all staff, including contractors, are trained as specified in the training requirements listed at (HIV/STD Security Training Plan) and as otherwise specified by DSHS.
- The LRP will maintain a list of persons who have been granted authorization to view and work with confidential information. The LRP will review authorized user lists annually.
- The LRP will ensure that this policy is reviewed annually and that evolving technology is reviewed on an on-going basis to make certain that the program's data remains as secure as possible.
- The LRP will be responsible for re-evaluating and re-assigning access to confidential information when an employee changes position within the HIV/STD program.

8.0 Procedures

All external programs must maintain written procedures for maintaining the security of confidential information. Such procedures must include the elements listed in the applicable activity-specific procedures for HIV/STD Surveillance, Public Health Follow-Up, the Medication Program and the Medical Monitoring Project.

9.0 Revision History

Date	Action	Section
07/02/08	This is a new policy	

Texas Department of State Health Services
Data Release Agreement

_____ (printed name) has been identified as the Responsible Party for assuring security and confidentiality of the data released to them by the Texas Department of State Health Services (DSHS).

Instructions
Persons in receipt of data from the HIV/STD Program must initial next to each item below to indicate agreement with the terms.

Data Release

_____ Attach 1) an outline of the purpose of the data requested and 2) an itemized list of the data fields requested. ***Include the fewest number of fields required to accomplish the task.***

_____ Access to the data will be limited to the minimum number of staff needed to accomplish the task. Each of these staff members have been provided training on general standards of confidentiality, and have on file a signed copy of the Texas Health and Human Services Commission Confidentiality Statement. A list of individuals who will have access to the data is included in this request.

_____ All reports or results released from use of this data will only be in aggregate form and will adhere to the attached DSHS HIV/STD Data Release Policy.

Physical Security

_____ Data will be stored in a locked cabinet located in a locked room.

_____ Access to computer(s) containing the data will be password protected.

_____ Data will be encrypted when not located on the password-protected computer.

_____ Hard copy output of individual records or data that do not satisfy the guidelines outlined in the HIV/STD Data Release Policy will be kept in a secure area and will be shredded as soon as possible.

Project Completion

_____ Estimated date of project completion: _____.

_____ The data, as well as any additional data files created, will be permanently erased and wiped after completion of the project. The DSHS Local Responsible Party or designee will be notified upon completion.

_____ Manuscripts or reports resulting from analysis of the data will be provided to the DSHS Local Responsible Party.

Signature below indicates the Responsible Party agrees to the terms of this data release agreement:

_____ _____

Responsible Party Signature Date

_____

Agency or Institution

_____ _____

DSHS HIV/STD Epidemiology and Surveillance Branch Manager Date

BREACH REPORT FORM

Section 1: Initial Report (To be completed by the DSHS staff member receiving the initial notice of the suspected breach.)

Type of Breach: ☐ **Unauthorized Release of Information** ☐ **Unauthorized Access to Information**

Date and Time of Breach: Date: **Time:** *(Approximate if Unknown)*

Location Where the Breach Occurred:

Organization Name	*Address*	*City*	*State*

Type of Data that was compromised:
☐ **Personally Identified Individual Record-Level Data**
☐ **Pseudo-anonymized Data**
☐ **Aggregate Data**

Means of Unauthorized Access or Release of Information:

☐ Building security	☐ Field investigation	☐ Workstation	☐ Handling confidential mail
☐ Telephone	☐ Electronic data storage	☐ Electronic data transmission	☐ Faxing (facsimile) records
☐ Email	☐ Routine sharing of data	☐ Laptops	☐ Removable storage devices
☐ GPS systems	☐ Personal storage devices	☐ Wi-Fi/blue tooth	☐ Other:_____

Person Submitting This Report:	
Name:	Agency/Affiliation:
Work Phone:	E-Mail Address:
Date Submitted:	Time Submitted:
Signature:	Title:

Person Who Released the Unauthorized Information:	
Name:	Agency/Affiliation:
Work Phone:	E-Mail Address:
Title:	

Section 1: Initial Report (cont.)

Describe the Suspected Breach that Occurred:
Describe Contributing Causes to the Incident:

Section 2: Security Team Closing Report (To be completed by the Security Team.)

Did a breach in protocol occur? ☐ Yes or ☐ No

Did a breach in confidentiality occur? ☐ Yes or ☐ No

Was the breach due to negligence or purposeful in nature? ☐ Negligence or ☐ Purposeful

Has confidential information been compromised? ☐ Yes or ☐ No ☐ Unknown

If yes, what information has been compromised?

If no, please elaborate on your response?

Security Team Conclusions:

Immediate Recommendations:
(corrective actions)

Long-Term Recommendations:
(corrective actions)

Is follow-up action needed: ☐ Yes or ☐ No

Section 3: Follow-up Report (To be completed by the Group Manager/External LRP.)

Were any disciplinary actions or corrective actions taken to prevent the breach from occurring again? ☐ Yes or ☐ No

If yes, then please describe the disciplinary and/or corrective actions that have been taken monthly to prevent the breach from occurring again.

This incident has been investigated, the proper officials have been notified, and the corrective actions have been implemented in the event a breach has been confirmed.

Security Team Member Signature: ***(Group Manager/External LRP)***	**Date:**
Typed Name:	

I have reviewed and approved the resolution of this investigation and actions taken.

Internal LRP Signature:	**Date:**
Typed Name:	
Internal LRP Signature:	**Date:**
Typed Name:	

INSTRUCTIONS TO FILL OUT BREACH REPORT FORM
Sections of the Breach Report Form are in bold font and instructions are in normal font. Please complete this form for all suspected breaches that occur. (A suspected breach is defined as an alleged infraction or violation of a standard that may result in unauthorized disclosure of confidential information.) Please refer to the HIV/STD Breach of Confidentiality Response Policy for more information on method and timing of submittal of this form.

Section 1: Initial Report:

Per the HIV/STD Program Breach of Confidentiality Response Policy, the DSHS staff member who received the initial notice of the suspected breach will document the incident by completing *Section 1: Initial Report* of this form.

Type of Breach

Put a check mark in the box that closest describes the type of breach that may have occurred.

☐ **Unauthorized Release of Information**
Accidental or purposeful release of data– verbally, electronically, or by paper medium - to an entity or person that by law does not have a right or need to know.

☐ **Unauthorized Access to Information**
Purposeful access of data - either in person or electronically – by an entity or person that by law does not have a right or need to know.

Date and Time of Breach

Date: _____ **Time:** _____
Type in the date and time the suspected breach actually occurred. If uncertain of the exact date or time, use a best estimate.

Location Where the Breach Occurred

Organization Name_____
Type in the Agency, Unit, Company, Group or Other Title that best describes the business affiliation of the location where the suspected breach occurred.

Address_____ **City**_____ **State**_____
Type in the physical address of where the suspected breach occurred, including: street, building or room numbers, suites, etc.

Type of Data that was compromised

Put a checkmark in the box that best describes the type of data that may have been breached:

☐ **Personally Identified Individual Record-Level Data:** Defined in the *Release of HIV/AIDS and STD Data Policy* as: Individual patient records that contain personal identifiers. A personal identifier is a datum or collection of data which allows the possessor to determine the identity of a single individual with a specified degree of certainty. A personal identifier may permit the identification of an individual within a given database. Bits of data, when taken together, may be used to identify an individual. Personal identifiers may include name, address or place of residence, social security number, telephone number, fax number, and exact date of birth.

☐ **Pseudo-anonymized Data:** Defined in the *Release of HIV/AIDS and STD Data Policy* as: Individual record-level data which has been stripped of personal identifiers (e.g., name, address, social security number) but may contain potentially identifying information (e.g., age, sex, race/ethnicity, locality information) that when combined with other information may identify an individual. If the combining of information could identify an individual, these data are considered confidential.

☐ **Aggregate Data:** Defined in the *Release of HIV/AIDS and STD Data Policy* as: Data which are based on combining individual level information. Aggregate data may contain potentially identifying information, particularly if the aggregated data are very detailed or for a small subset of individuals.

Means of Unauthorized Access or Release of Information

Put a checkmark in the box (es) that best describe the method(s) by which the suspected breach occurred. See the *HIV/STD Confidential Information Security Policy* for more specific information regarding each of these methods.)

☐ Building security	☐ Field investigation	☐ Workstation	☐ Handling confidential mail
☐ Telephone	☐ Electronic data storage	☐ Electronic data transmission	☐ Faxing (facsimile) records
☐ Email	☐ Routine sharing of data	☐ Laptops	☐ Removable storage devices
☐ GPS systems	☐ Personal storage devices	☐ Wi-Fi/blue tooth	☐ Other:_____

Contact information for the persons involved with the suspected breach:

Person Submitting This Report

Name: _____ **Agency/Affiliation:**_____
Full name of the DSHS staff reporting the suspected breach (on behalf of the person who witnessed or discovered the suspected breach); and the Agency, Unit, Company, Group or Other Title that best describes their business affiliation.

Work Phone_____ **E-Mail Address**_____
Telephone number and E-mail address where this person can be reached during daytime hours.

Date Submitted_____ **Time Submitted**_____
Date and the Time of Day the Breach Report Form was filled out and submitted.

Signature_____ **Title**_____
Signature and job title of the person that is reporting the suspected breach.

Person Who Released the Unauthorized Information

Name: _____ **Agency/Affiliation:**_____
Full name of the person suspected of releasing unauthorized information and
the Agency, Unit, Company, Group or Other Title that best describes their business affiliation.

Work Phone_____ **E-Mail Address**_____

Telephone number and E-mail address where this person can be reached during daytime hours.

Title_____

Job title of the person suspected of releasing unauthorized information.

Describe the Suspected Breach of Protocol that Occurred

Write a brief description of the suspected breach as it occurred. Include how the breach was discovered and any other relevant information.

Describe Contributing Causes to the Incident

Write the specific cause(s) that contributed to the suspected breach. (For example, policies and procedures were not followed, policies and procedures were not enforced, and/or training was not adequate.)

Section 2: Security Team Closing Report

Per the HIV/STD Program Breach of Confidentiality Response Policy, the Security Team will be responsible for completing *Section 2: Security Team Closing Report* of this form.

In answering the following questions see the *HIV/STD Breach of Confidentiality Response Policy* for definitions.

Did a breach in protocol occur? ☐ Yes or ☐ No

Did a breach in confidentiality occur? ☐ Yes or ☐ No

Was the breach due to negligence or was it purposeful in nature? ☐ Negligence or ☐ Purposeful

Has the confidential information been compromised? ☐ Yes ☐ No ☐ Unknown

If yes, what information has been compromised?

If no, please elaborate on your response.

Security Team Conclusions/Recommendations:

Conclusions:

Write the conclusions set forth by the Security Team.

Immediate Recommendations:

Write the immediate corrective actions to be taken.

Long-Term Recommendations:
Write the long-term corrective actions to be taken.

Is follow-up action needed: ☐ **Yes or** ☐ **No**
Select only one response.

Section 3: Follow-up Report

This section is to be completed by the Group Manager/External LRP.

Were any disciplinary actions or corrective actions taken to prevent the breach from occurring again?
☐ **Yes or** ☐ **No** (Select only one response.)

If yes, please describe the disciplinary and/or corrective actions that have been taken monthly to prevent the breach from occurring again. (Provide a monthly update to the LRP until the LRP determines no further action is needed and the LRP closes out the report.)

Sign-off from Security Team Member(s)

This incident has been investigated, the proper officials have been notified, and the corrective actions have been implemented in the event a breach has been confirmed.

Security Team Member Signature: _____ **Date:**_____
(Group Manager/External LRP) (Signature)

Typed Name:_____

(Sign-off from Management)

I have reviewed and approved the resolution of this investigation and actions taken.

Internal LRP Signature: _____ **Date:**_____
(Signature)

Typed Name:_____

Internal LRP Signature: _____ **Date:**_____
(Signature)

Typed Name:_____