HIV Security and Confidentiality Policy

Alabama Department of Public Health
Office of HIV Prevention and Care

Certification of Compliance with NCHHSTP Data Security and Confidentiality Standards

Alabama's HIV Surveillance Program is in full compliance with the National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention's (NCHHSTP) Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action (2011).

Contact Person:
Danita Crear, DrPH, Director
HIV Surveillance
Phone: (334) 206-6499
E-mail: Danita.Crear@adph.state.al.us

Contents

I. INTRODUCTION

The Alabama Department of Public Health (ADPH), HIV Surveillance Branch is responsible for implementing and operating a comprehensive HIV surveillance program to reduce the spread of HIV infection and its impact on Alabama residents. Maintaining security and confidentiality of HIV data is central to HIV surveillance acceptability and success. Appropriate collection, storage, and use of sensitive HIV information between programs providing integrated and comprehensive services for HIV prevention are essential. Standardized data security and confidentiality procedures for handling HIV information across all public health programs are necessary. This document serves as the official HIV Security and Confidentiality Policy and is intended to provide guidelines for management of confidential HIV information within the context of the state's surveillance activities.

Alabama's HIV Security and Confidentiality Policy is in full compliance with the National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention's (NCHHSTP) Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs. This policy follows the Ten Guiding Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality listed below.[1]

10 Guiding Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality

1. Public health data should be acquired, used, disclosed, and stored for legitimate public health purposes.
2. Programs should collect the minimum amount of personally identifiable information necessary to conduct public health activities.
3. Programs should have strong policies to protect the privacy and security of personally identifiable data.
4. Data collection and use policies should reflect respect for the rights of individuals and community groups and minimize undue burden.
5. Programs should have policies and procedures to ensure the quality of any data they collect or use.
6. Programs have the obligation to use and disseminate summary data to relevant stakeholders in a timely manner.
7. Programs should share data for legitimate public health purposes and may

[1] Centers for Disease Control and Prevention. Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action. Atlanta (GA): U.S. Department of Health and Human Services, Centers for Disease Control and Prevention; 2011. (Adapted from: Lee, LM, Gostin, LO. Ethical collection, storage, and use of public health data: a proposal for national privacy protection. JAMA 2009;302:82–84)

establish data-use agreements to facilitate sharing data in a timely manner.

8. Public health data should be maintained in a secure environment and transmitted through secure methods.
9. Minimize the number of persons and entities granted access to identifiable data.
10. Program officials should be active and responsible stewards of public health data.

II. LEGAL AUTHORITY

Federal Regulations

At the national level, the enhanced HIV/AIDS Reporting System (eHARS) is protected by the Federal Assurance of Confidentiality of Public Health Service Act, 42 U.S.C. 242k and 242m(d), prohibiting disclosure that could be used to directly or indirectly identify patients.

State Reporting Regulations

Each physician, dentist, nurse, medical examiner, hospital administrator, nursing home administrator, laboratory director, school principal, and day care center director is required to report all conditions (including any test or series of tests indicative of HIV infection, CD4 results, and viral loads, detectable and undetectable) per the Rules and Regulations concerning communicable diseases published in the Public Health Laws of Alabama. Health care providers are protected from any civil liability for reporting under Code of Ala, 1975 §22-11A-1 and 22- 11A-2. There are no exemptions to reporting for health care professionals or laboratories (i.e., clinical trial, research laboratories), per rules, regulations, and state statutes.

Penalties for Unauthorized Release of Information

As defined in the Code of Ala, 1975 § (22-11A-22), penalties for unauthorized releases of any communicable disease information, including HIV information, are classified as a Class C misdemeanor. Breach of security and confidentiality by a public health employee may result in suspension, demotion, or termination based on the severity of the offense. Severity of offense and disciplinary action for public health employees with access to HIV data is determined by the Overall Responsible Party (ORP). Federal penalties for breach of confidentiality of HIV surveillance data may include a reduction or loss of federal funding for Alabama's HIV Surveillance Project.

III. ACCESS AND ROLES

The HIV Surveillance branch is the administrative headquarters for all state surveillance activities conducted under Alabama's HIV Surveillance Project. The HIV Surveillance Branch is composed of public health employees based at the central office in Montgomery, the Jefferson County Health Department in Birmingham, and the Madison County Health Department in Huntsville. HIV Surveillance staff conduct investigations with health care providers and testing laboratories while STD Disease Intervention Specialists (DIS) perform patient investigations and partner services for newly diagnosed HIV infections.

Access to HIV Surveillance Data

Access to the HIV Surveillance database (eHARS) and electronic scanned copies of HIV Surveillance records (Laserfiche) is limited to HIV Surveillance staff, STD DIS, and designated information technologists. Hard copies of HIV Surveillance records are stored in a locked file room within the Office of HIV Prevention and Care (OHPC) and archived annually to the State Records Office. Annually, a list of the current personnel with designated job titles having access to HIV surveillance data is maintained by the HIV Surveillance Director.

IV. OVERALL RESPONSIBLE PARTY (ORP)

The OHPC Director serves as the ORP for the Office of HIV Prevention and Care. The ORP is ultimately responsible for implementing and enforcing security and confidentiality standards governing appropriate collection, storage, and use of HIV data. The ORP exercises authority to make decisions about the overall HIV surveillance operation, affecting how data is collected, stored, analyzed, released, and disposed of, as well as which programs are authorized to access surveillance data for public health purposes. The HIV Surveillance Director recommends access privileges to the ORP for approval. The ORP annually certifies that Alabama's HIV Surveillance Program is in compliance with the National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention's (NCHHSTP) Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs.

V. DATA RELEASE

All data is released in accordance with the Code of Ala, 1975 §Code of Ala, 1975 §22-11A-22 and the HIV Data Release Policy. The HIV Data Release Policy, approved by the state ORP, lists specific protocols and policies for the release of HIV information. Questions pertaining to release of HIV information should be directed

to the ORP or HIV Surveillance Director.

HIV Statistics
HIV Statistics are disseminated on the ADPH website: http://alabamapublichealth.gov/hiv. Great caution is taken in the release of numerical, small cell data that could either directly or indirectly lead to the identification of a person infected with HIV. Small cell data of five or less are not released. Several independent variables (e.g., risk factor, race, age) could lead to the direct or indirect identification of a person with HIV and are carefully evaluated before release.

Data Requests
Data requests require completion of a signed HIV Data Request Agreement. As with published statistics, small cell data of five or less cases are not released. De-identified county-level analysis datasets may be provided to researchers for the analysis of HIV surveillance data upon signing the HIV Data Request Agreement. Unusual requests for HIV surveillance data will be referred to the ORP or legal counsel.

State and Local Prosecuting Agencies
According to state statute, communicable disease records are not subject to subpoena; ADPH does not release HIV surveillance information to law enforcement officials (e.g., defense attorneys, prosecuting attorneys, and detectives) under any circumstances. Court orders for HIV surveillance data will be referred to the ORP and legal counsel.

HIV Case Information
Case report information pertaining to a specific HIV case may be released to the person who completed the case report form, the diagnosing physician or his designee (e.g., nurse or other contact, with prior verbal consent from the physician), or the OHPC Director (ORP).

Information may also be released to authorized out-of-state surveillance staff for investigating patients within their jurisdiction. Each state maintains a list of authorized HIV surveillance staff on the secure Council of State and Territorial Epidemiologists (CSTE) HIV Contact Board. The Contact Board will be checked prior to releasing HIV personally identifiable information.

VI. DATA SHARING AGREEMENTS

Confidential information may be released to programs within ADPH Central Office requiring such information to perform program job responsibilities (i.e., HIV, STD, and Tuberculosis Programs). Data sharing with programs outside ADPH Central Office will be considered for the sole purpose of reengagement efforts described in the Data to Care strategy supported by the Centers for Disease Control and Prevention (CDC), HIV Incidence and Case Surveillance Branch (HICSB).

STD Prevention and Control
STD Disease Intervention Specialists (DIS) conduct patient field investigations and partner notification services for newly diagnosed HIV infections. HIV Surveillance staff may provide DIS with demographic and clinical information needed to perform effective field investigations.

Through partner notification, DIS can potentially identify new cases of HIV infection through testing. When investigations cross jurisdictional lines, STD staff shares information with out-of- state STD Control programs. Exchange of information between HIV surveillance staff and DIS staff is bilateral and occurs at the state and local levels.

Tuberculosis (TB) Control
Linkage between the HIV and TB case registries is conducted annually by the HIV Surveillance Director. Name, date of birth, sex, race, ethnicity, social security number, and HIV status of all confirmed TB cases are provided to the HIV Surveillance Director and matched against HIV cases reported in the HIV Surveillance database (eHARS). If an individual is co-infected with HIV and TB, the patient record is updated in eHARS and the TB case registry to capture HIV and TB co-infection, the TB RVCT number, and the HIV StateNo. HIV data are not directly accessible to the TB program, however individual information is provided during TB investigations upon request.

Data to Care
Any program approved to receive HIV data for the purpose of re-engaging HIV clients into care must be in full compliance with the NCHHSTP Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs. To be considered, programs must provide a detailed plan of how data will be used to conduct re-engagement outreach activities and how the security and confidentiality of clients will be protected.

Data sharing with programs outside ADPH Central Office requires approval of the ORP, HIV Surveillance Director, State Health Officer, and legal counsel. A Memorandum of Understanding (MOU) must be completed between ADPH and the program requesting data. The HIV Surveillance branch will provide only the minimum data required to conduct re-engagement activities.

VII. VERBAL DATA COMMUNICATION

Routine verbal communications requiring the sharing of confidential, identifiable data with other project areas—both intrastate and interstate and providers, laboratories, and other internal and external entities—are to occur discreetly in secured, private areas so as to not be overheard by others.

Desk Telephone

Patient identifying information is communicated via telephone to perform routine HIV surveillance activities. Incoming calls are answered with generic identifiers (e.g., "Department of Public Health, this is Joe"), without any direct reference to HIV. Phone calls regarding case reports are taken only by HIV Surveillance staff. If visitors are in the work area when calls are received, the visitors are asked to leave. Confidential information is shared over the phone with individuals authorized to access HIV surveillance information. Any out-of-state HIV Surveillance staff is verified on the secure Council of State and Territorial Epidemiologists (CSTE) HIV Contact Board. Techniques such as call back verification are utilized to verify authorized individuals reporting HIV data. HIV Surveillance staff discuss confidential information so as not to be overheard by others, release information to only individuals with a need-to-know, and always use utmost discretion. Messages with patient identifiers are not left on voice mail systems.

Cellular Phone

Cellular phone transmission is not secure. Patient identifying information is never used during cellular phone calls. Callers refer to specific individuals by eHARS ID or some other reference that is familiar to the recipient of this information. If patient identifying information must be shared, the caller will return the call from a land line telephone. Exception. Exchanging confidential information via cellular phone may be permissible when conducting record searches with out of state jurisdictions whose staff are working remotely using state issued cellular phones.

VIII. PHYSICAL DATA SECURITY

Restricted Access Area Security

The OHPC is located on the 12th floor of the Retirement Systems of Alabama Tower, a restricted card access floor with one staff controlled main entrance. Card access is available to approved staff during normal working hours (defined as 7:00 am to 6:00 pm., Monday through Friday). Facility management, including maintenance and cleaning crews, also have access to the floor, but not to offices where HIV Surveillance records are stored.

HIV Surveillance Branch

The HIV Surveillance Branch is housed in an open bay area with other programs within the OHPC including the HIV Prevention and the Ryan White Programs. Identification badges are required to be worn by all Alabama Department of Public Health employees. Visitors to the OHPC are required to sign in, are issued a visitor's badge, and are escorted to their destination. Administrative support telephones appropriate staff to inform them of the visitor's presence. When visitors are present, patient identifying information is removed from view (e.g., clear computer screens).

HIV surveillance activities are conducted in the OHPC. Five of the six computer terminals conducting surveillance activities are located in cubicles; the sixth terminal is located in the office of HIV Surveillance Director. Confidential information is not left unattended in common access areas and is retrieved immediately upon copying/printing. Hard copy documents are concealed or locked up when Surveillance staff are absent from individual workstations, even for brief periods of time. Locked filing cabinets containing HIV surveillance information are large and heavy enough to render them immobile and are located in a locked file room within the OHPC. Keys to the filing cabinets are maintained by the HIV Surveillance Director.

Field Investigations

Field investigations and medical record reviews are conducted as discreetly as possible in secure, private areas. Confidential information is never left in public or general access areas. Field investigations may require line lists to perform routine HIV surveillance activities. Patient identifying information transported to the field does not contain reference to HIV infection and is limited to name, date of birth, address, date of test, and coded risk information. Information is carried in secured briefcases when performing field activities and is limited to investigations performed that day, with all information returned to the office at the close of each business day. Briefcases should not be left unattended. Overnight travel or other scenarios precluding return of patient identifying information by close of business requires approval of the HIV Surveillance Director and/or OHPC Director. During these scenarios, confidential information will be stored in appropriate places (e.g., locked

hotel rooms, private residences).

Resignation
Employees must sign a resignation list certifying they have returned all files, documents, office and file keys, identification badges, phone cards, voice mail passwords, tablets, laptops, database user ids and passwords, and any other office equipment to their supervisor. The supervisor initials the list indicating possession of each item. Failure to comply with State resignation procedures results in delay of the employee's final paycheck.

IX. ELECTRONIC DATA SECURITY

HIV Surveillance Database (eHARS)
The Enhanced HIV/AIDS Reporting System (eHARS) is maintained on a local area network (LAN) by designated information technologists. Approved HIV and STD staff (STD read only) may access eHARS between the hours of 7:00 AM -6:00 PM Monday through Friday. Passwords at start-up and screen savers are utilized to maintain security of eHARS while it is in Back-up of eHARS is performed daily. Saved data is encrypted and stored in the secure server vault within ADPH for one month.

Laserfiche
Scanned copies of HIV Surveillance data are uploaded to Laserfiche, a secure, web-based electronic filing system in compliance with the NCHHSTP Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs (2011). Laserfiche interfaces directly with eHARS while being maintained on a LAN by designated information technologists. It is utilized by multiple HIV Surveillance programs nationwide. Approved HIV Surveillance and Alabama's AIDS Drug Assistance Program (ADAP) staff may access Laserfiche.

Passwords at start-up and screen savers are utilized to maintain security of Laserfiche while it is in use. Technical support is provided via remote user access by designated Laserfiche information technologists who are required to complete annual HIV Security and Confidentiality Training and have current signed confidentiality agreement forms on file with the HIV Surveillance Director.

PC Workstation Security
All state and local staff authorized to access HIV personally identifiable information must be responsible for protecting his or her workstation (hardcopy files and electronic computer files) associated with confidential HIV surveillance data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Passwords in all surveillance jurisdictions are at least a minimum of 7 characters comprised of numbers and letters. Surveillance staff logs off the computer at the end of each day or when leaving the workstations. Anti-virus software is installed on the network server and staff must take care not to infect surveillance software with computer viruses. All disks and computer hard drives are wiped prior to destruction.

X. DATA TRANSMISSION

Data Transmission
The CDC requires data transmissions for activities funded through Alabama's HIV Surveillance Project. Data related to Core, Incidence, and Molecular HIV Surveillance are transmitted to CDC on a monthly or quarterly basis utilizing the Secure Access Management Services (SAMS). Data transmissions are encrypted meeting the standards detailed in Federal Information Processing Standards (FIPS) Publication 197, Advanced Encryption Standard (AES). Patient identifying information is not transmitted to the CDC.

Incoming Mail
Reporting sources are instructed to address mail to the Office of HIV Prevention and Care with Attention: HIV Surveillance Director and to mark the envelope "CONFIDENTIAL" and/or "TO BE OPENED BY ADDRESSEE ONLY". Physicians and other case reporters are provided return envelopes stamped "confidential" for submitting case reports. Return envelopes have no direct reference to HIV. Mail is delivered to the office at least once each working day via courier.

Only designated HIV surveillance staff opens program mail. The OHPC Director or the HIV Surveillance Director is notified of all mail routed to the incorrect health department program and appropriate public health employees or providers notified to prevent recurrence.

Outgoing Mail
Outgoing mail containing patient identifying information is placed in two sealed envelopes. The inner envelope is marked "CONFIDENTIAL" and "To Be Opened by Addressee Only" and sealed with package tape. The outer envelope is sealed and has no direct or indirect reference to HIV.

Facsimile
Facsimile (fax) is not used to send patient identifying information. Receipt of patient identifying information via fax is discouraged. Exception. When necessary, faxes are received on the secure HIV Surveillance Right Fax Server.

E-mail
E-mail is not used to transmit Patient identifying information. Receipt of confidential HIV information via e-mail is discouraged. Electronic morbidity reports submitted through the Detect, Test, and Report Notifiable Disease Awareness Campaign STD/HIV Morbidity Card and REPORT card feed into an encrypted e-mail account accessible on the secure ADPH server. This e-mail account is monitored by the OHPC with HIV morbidity reports forwarded to the HIV Surveillance Branch. The University of Alabama (UAB) Hospital Laboratory transmits encrypted HIV laboratory reports to the HIV Surveillance Director through UAB Medicine's secure e-mail server. The Surveillance Director has a secure account to download encrypted files from UAB. HIV data is not uploaded to this account. Exception. E-mail sent within the ADPH firewall system may be permissible so long as the files are password encrypted in accordance with federal encryption standards prior to being transmitted using ADPH encrypted lotus notes software. All encryption methods must meet standards detailed in Federal Information Processing Standards (FIPS) Publication 197, Advanced Encryption Standard (AES). (See http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf .) Passwords to decrypt files must be shared via telephone and cannot be e-mailed.

XI. DISPOSAL OF DATA

Retention of Hard Copy Files
The HIV Surveillance Branch retains hard copy files of HIV surveillance information for ten years after the death of the patient. In 2014, hard copy files were archived at the State Records Office. Subsequent hard copy information is archived annually and stored in locked filing cabinets in a locked file room within the OHPC until archived as described above.

Physical Data Security
Any notes or follow-up information are stored with the case report and shredded using a crosscut shredder when no longer needed. Daily shredding of documents takes place in the secure HIV Surveillance of the OHPC area using a micro-crosscut shredder. The contents of the shredder are bagged and disposed by the HIV Surveillance staff. Large shredding projects are managed by a contract company. Until shredding occurs, documents are stored in locked shredding bins located in the secure HIV Surveillance area.

Electronic Files and Equipment
All disks, computer hard drives, and jump drives are wiped clean prior to

destruction by designated information technologists.

XII. SECURITY BREACHES

The ORP is required to investigate any breach of data immediately; regardless of whether personal identifying information was released (PII). Any breach that results in the release of PII to unauthorized persons must be reported to the CDC, HICSB Project Office and the ADPH Security Officer by the ORP. Federal penalty for breach of confidentiality of HIV surveillance data may include a reduction or loss of funding for Alabama's HIV Surveillance Project.

Breach of security and confidentiality by a public health employee may result in suspension, demotion, or termination based on the severity of the offense. Severity of offense and disciplinary action for public health employees with access to HIV patient identifying information is determined by the ORP. The ORP is responsible for submitting an Automated Report of Incidents and Accidents (ARIA) documenting the disclosure. Consultation will take place with the compliance officer and the Department's General Counsel to determine whether a breach warrants reporting to local and state law enforcement agencies, and to determine warranted civil and criminal actions.

All state and local staff authorized to access HIV personally identifiable information are responsible for challenging attempted use of data by unauthorized users and are also responsible for immediately reporting all breaches or suspected breaches of confidentiality to the HIV Surveillance Director. The HIV Surveillance Director will then immediately notify the state ORP. Any potential breach of confidentiality within the OHPC results in appropriate disciplinary action under the authority of the ORP. The ORP collaborates with non-OHPC programs handling public health HIV patient identifying information whose employees breach confidentiality to initiate appropriate disciplinary action.

From time to time, security and confidentiality issues not specifically addressed in this policy may arise. Surveillance staff is responsible for notifying the HIV Surveillance Director for necessary guidance in these scenarios.

XIII. TRAINING

New Employee Orientation

Orientation of state and local staff authorized to access HIV personally identifiable information includes comprehensive training on security and confidentiality requirements and related procedures. Training is prioritized to ensure each employee fully understands the obligation and necessity of maintaining strict

security and confidentiality in all aspects of their work.

Training includes explanations of the federal assurance of confidentiality upon which HIV surveillance is based, how it is essential to program success both nationally and at the state level, and how any infractions can result in harm to individuals as well as damage the confidence of the public and reporting contacts. Alabama's state laws governing confidentiality of personally identifiable information and associated penalty for violation are reviewed with a copy of these laws provided during orientation. The confidentiality safeguards established within HIV Surveillance and specific office procedures that must be followed are provided.

Examples of ways to handle both routine and potentially compromising situations that may occur within the scope of each employee's duties are given. A signed agreement declaring no potential conflicts of interest related to employment is also required during orientation.

Annual Training and Reviews

All state and local staff authorized to access HIV personally identifiable information are required to complete annual HIV Security and Confidentiality Training. The training is available via the Department's web-based Learning Content Management System (LCMS) and is managed by the HIV Surveillance Director. Certificates of completion are maintained by the HIV Surveillance Director. Security and confidentiality reviews are conducted annually at the employee's performance appraisal. Updates allow for sharing of information and experiences regarding security and confidentiality, including discussion of new policies, review of existing policies, review of program requirements, discussion of areas of perceived weakness within the statewide program, and discussion of individual penalties for unauthorized disclosure of confidential information.

Confidentiality Agreement

All state and local staff authorized to access HIV personally identifiable information must sign a confidentiality agreement acknowledging compliance with Alabama's HIV Security and Confidentiality Policy upon hire and annually thereafter. Written acknowledgement pledging to maintain security and confidentiality in accordance with departmental practices and procedures includes that worker can be sued for breaches, in addition to liability for criminal penalties for disclosure. A copy of the signed confidentiality agreement is maintained by the HIV Surveillance Director.

Federal Trainings

At least one HIV surveillance staff, preferably the HIV Surveillance Director, attends all CDC recommended or required security and confidentiality trainings.

XIV. POLICY REVIEW

The HIV Security and Confidentiality Policy is reviewed annually to ensure security practices are current and in line with evolving technology. Proposed changes to information systems technology require discussion between the HIV Surveillance Director and Division of Information Technology to ensure security and confidentiality of electronic HIV surveillance data are maintained. The HIV Surveillance Director monitors statewide progress toward meeting CDC Program Requirements. HIV Surveillance activities conducted by STD Partner Services at satellite offices are reviewed on an annual basis to ensure compliance with program requirements.

APPENDIX

GLOSSARY

Access
Ability or means needed to read, write, modify, or communicate data/information.

Advanced Encryption Standard (AES)
This standard specifies the algorithm that can be used to protect electronic data and is issued by the National Institute of Standards and Technology (NIST). Publication 197 of the Federal Information Processing Standards (FIPS) contains the specifications of the AES, which can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back to its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. NIST publication 140-2 details the protection of a cryptographic module within a security system necessary to maintain the confidentiality and integrity of the information protected by the module.

AIDS
Acquired Immune Deficiency Syndrome. The term AIDS is being phased out and replaced with Stage 3 HIV infection.

Analysis Dataset
Set of aggregated data created by removing identifying information (e.g., names, addresses, ZIP codes, telephone numbers) so that the data cannot be linked to a specific person but can still be used for data analysis.

Authorized Access
As determined by the ORP or designee, permission granted to an authorized person to see confidential or potentially identifiable public health data, based on the public health role of the individual and their need to know.

Breach of Confidentiality
A compromise, disclosure, acquisition, access, or loss of control of personally identifiable information (PII) that results in the release of PII to unauthorized persons (i.e., employees or members of the general public).

Breach of Personally Identifiable Information
Defined by OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Office of HIV Prevention and Care (OHPC)
Performs statewide surveillance for HIV, including HIV partner counseling, testing, and referral services as well as HIV disease education and prevention.

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

Confidentiality
Protection of personal information collected by public health organizations. The right to such protection is based on the principle that personal information should not be released without the consent of the person involved, except as necessary to protect public health.

Confidentiality Agreement
A contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes but wish to restrict access to by third parties. It is a contract through which the parties agree not to further disclose information covered by the agreement.

Data Dissemination
Any mechanism by which data (typically in aggregate form) are made available to

users. Includes mechanisms whereby data is released to users as well as mechanisms whereby data is made available without being released.

Data Encryption Standard (DES)
Algorithm that encrypts and decrypts data in 64-bit blocks. Since the DES always operates on data blocks of equal size and uses both permutations and substitutions in its algorithm, it is both a block cipher and a product cipher.

Data Sharing
Granting certain individuals or organizations access to data that contain personally identifiable information with the understanding that personally identifiable or potentially identifiable data cannot be re-released further unless a special data-sharing agreement governs the use and re- release of the data and is agreed upon by the receiving program and the data provider(s).

Data-Sharing Agreement
Mechanism by which a data requestor and data provider can define the terms of data access that can be granted to requestors.

Data Release
Dissemination of data either in a public-use file or as a result of an ad hoc request which results in the data steward no longer controlling the use of the data. Data may be released in a variety of formats including, but not limited to, tables, microdata (person records), or online query systems.

Disclosure
Occurs when identifiable information concerning an individual is made known to a third party. Disclosures may be authorized (as when a person has consented to the information being so divulged), unauthorized (as when information is intentionally revealed to a party not consented to by the person), or inadvertent (as when a tabulation or file is unintentionally made available to the public that reveals or can be used to reveal personal information).

Disease Intervention Specialist (DIS)
STD Partner Services staff responsible for patient investigation and partner notification of newly diagnosed HIV infections.

eHARS (Enhanced HIV/AIDS Reporting System)
National and statewide database for conducting HIV case surveillance.

Encryption
Manipulation or encoding of information so that only parties intended to view the information can do so. The most commonly available encryption systems involve public key and symmetric key cryptography. In general, for both public and symmetric systems, the larger the key, the more robust the protection.

HIV
Human Immunodeficiency Virus.

HIV Surveillance Branch
Work unit responsible for conducting and overseeing all statewide HIV surveillance activities conducted under Alabama's HIV Surveillance Project.

Immediately
With respect to reporting all breaches or suspected breaches of confidentiality (whether local health department to state health department or state health department to CDC), immediately is defined as within the same working day. If an event occurs late in a working day, the statewide ORP is to be notified as soon as possible after the event occurs.

Need-to-know Access
Access to data granted to a specific person on a case-specific basis where exceptional circumstances exist that are not stipulated in program policies. This type of access should be reserved for unusual situations and granted only after careful deliberation by the ORP.

Non-public Health Use of Data
Release of data that are either directly or indirectly identifying to the public; to parties involved in civil, criminal, or administrative litigation; to non-public health agencies of the federal, state, or local government; or for commercial uses.

Overall Responsible Party (ORP)
The OHPC Director is ultimately responsible for the security and confidentiality of HIV personally identifiable information. This official has the authority to make decisions about program operations that may affect programs accessing or using

the data and serves as the contact for public health professionals regarding security and confidentiality policies and practices. The ORP is responsible for protecting data as they are collected, stored, analyzed, and released and must certify annually that all security program requirements are met.

Personally Identifiable Information (PII)

As defined by National Institute of Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), available at http://csrc.nist.gov/publications/: "Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

Physical Access Controls

Physical barriers such as locked doors, sealed windows, password-protected keyboards, entry logs, guards, etc., used to help limit access to confidential information.

Public Health Surveillance

The ongoing, systematic collection, management, analysis, and interpretation of health-related data followed by their dissemination to those who need to know in order to: 1) monitor populations to detect unusual instances or patterns of disease, toxic exposure, or injury; 2) act to prevent or control these threats; and 3) intervene to promote and improve health. The term applies to both electronic and paper-based systems.

Public Health Data Use (See Also Legitimate Public Health Purpose)

Includes the variety of ways public health data may be used to achieve public health goals/purposes. A principal public health data use at state and federal levels is for epidemiologic monitoring of trends in disease incidence and outcomes. This includes collection of data and evaluation of the collection system, as well as the dissemination of aggregate trends in incidence and prevalence by demographic, geographic, and behavioral risk characteristics to assist the formulation of public health policy and direct intervention programs. Public health data uses may also include data used to initiate or provide treatment and prevention services.

Records Retention Policy
A policy that stipulates how long paper and electronic records should be kept before they can be archived or destroyed.

Role-based Access
Access to specific information or data granted on the basis of a person's job status or authority. This control mechanism protects data and system integrity by preventing access to unauthorized applications. Granting access based on roles within an organization, rather than by individual users, simplifies an organization's security policy and procedures and helps avoid granting need-to-know access to individuals.

Secure Area
Workspace with physical access controls in which confidential data are kept and/or used with access granted only to authorized persons. The configuration of a secure area depends on resource and other program considerations (e.g., availability of physical space, locks, file cabinets, walls, doors, and other barriers).

Security
Protection of public health data and information systems to prevent unauthorized release of identifying information and accidental loss of data or damage to the systems. Security includes measures to detect, document, and counter threats to data confidentiality or the integrity of data systems.