Attachment K. *Technical Guidance for HIV/AIDS Surveillance Programs Volume III: Security and Confidentiality Guidelines*. Centers for Disease Control and Prevention; 2006.

Technical Guidance for HIV/AIDS Surveillance Programs

Volume III: Security and Confidentiality Guidelines

DEPARTMENT OF HEALTH AND HUMAN SERVICES
Centers for Disease Control and Prevention

Suggested Citation

Centers for Disease Control and Prevention and Council of State and Territorial Epidemiologists. *Technical Guidance for HIV/AIDS Surveillance Programs, Volume III: Security and Confidentiality Guidelines*. Atlanta, Georgia: Centers for Disease Control and Prevention; 2006.

The document is available at http://www.cdc.gov/hiv/surveillance.htm.

Contents — Security and Confidentiality

Notes

Contributors

This document, *Technical Guidance for HIV/AIDS Surveillance Programs*, was developed by the HIV Incidence and Case Surveillance Branch of the Division of HIV/AIDS Prevention, National Center for HIV, STD, and TB Prevention, Centers for Disease Control and Prevention in collaboration with the Council of State and Territorial Epidemiologists. The CDC/CSTE Advisory Committee provided oversight and leadership throughout the entire process. Workgroup contributors consisted of state and local health department representatives. Irene Hall, CDC, and Eve Mokotoff, CSTE, led the development.

Members of the CDC/CSTE Advisory Committee

CDC: Pamela Gruduah, Irene Hall, Martha Miller

CSTE: Gordon Bunch, California; Dena Ellison, Virginia; Jim Kent, Washington; Eve Mokotoff, Michigan; Stanley See, Texas

Chairs of Workgroups, CDC

Michael Campsmith, Data Analysis and Dissemination

Sam Costa, Security and Confidentiality

Irene Hall, Data Quality

Laurie Kamimoto, Electronic Reporting

Lata Kumar, Data Dictionary

Martha Miller, Overview

Kathleen McDavid, HIV Risk Factor Ascertainment

Ruby Phelps, Case Residency Assignment

Richard Selik, Death Ascertainment

Richard Selik, Record Linkage

Suzanne Whitmore, Perinatal and Pediatric Case Surveillance

CDC Contributors

Lori Armstrong, Mi Chen, Betsey Dunaway, John Gerstle, Kate Glynn, Irene Hall, Felicia Hardnett, David Hurst, Jennie Johnston, Danielle Kahn, Tebitha Kajese, Laurie Kamimoto, Kevin Lyday, Martha Miller, Andy Mitsch, Michelle Pan, Richard Selik, Amanda Smith, Damien Suggs, Patricia Sweeney, Kimberly Todd, Will Wheeler, Suzanne Whitmore, Irum Zaidi.

State and Local Health Department Contributors and Reviewers

Alabama: Anthony Merriweather, Danna Strickland; ***California-Los Angeles***: Gordon Bunch, Mi Suk Harlan, Virginia Hu, Ann Nakamura; ***California-San Francisco***: Ling Hsu, Maree Kay Parisi, Sandra Schwarcz; ***District of Columbia***: Gail Hansen, Kompan Ngamsnga; ***Florida***: Becky Grigg, Lorene Maddox; ***Illinois-Chicago***: Margarita Reina; ***Indiana***: Jerry Burkman; ***Iowa***: Randy Mayer; ***Louisiana***: Joseph Foxhood, Greg Gaines, William Robinson, Debbie Wendell, Amy Zapata; ***Massachusetts***: Maria Regina Barros;

Michigan: Elizabeth Hamilton, Nilsa Mack, Eve Mokotoff, Yolande Moore; ***Minnesota***: Luisa Pessoa-Brandao, Tracy Sides; ***New Hampshire***: Chris Adamski; ***New Jersey***: Wogayehu Afework, Linda Dimasi, Abdel Ibrahim, John Ryan; ***New York City***: Melissa Pfeiffer, Judy Sackoff; ***New York State***: Alexa Bontempo, Kathleen Brousseau, Donna Glebatis; ***Ohio***: Sandhya Ramachandran; ***Oklahoma***: Mark Turner; ***Pennsylvania***: Bonnie Krampe, Ming Wei; ***South Carolina***: Dana Giurgiutiu; ***Texas***: Thomas Barnabas, Dianna Highberg, Roy Reyna, Stanley See, Jan Veenstra; ***Virginia***: Dena Ellison; ***Washington***: Maria Courogen; ***Washington-Seattle & King County***: Amy Bauer, Jim Kent; ***Wisconsin***: Loujean Steenberg.

HIV/AIDS Surveillance Guidelines — Security and Confidentiality

Introduction

This document supersedes the October 1998 version of "Guidelines for HIV/AIDS Surveillance, Appendix C: Security and Confidentiality." It reflects CDC's recommendation as best practices for protecting HIV/AIDS surveillance data and information. It details program requirements and security recommendations.

These requirements, recommendations, and practices are based on discussions with HIV/AIDS surveillance coordinators, CDC's Divisions of STD Prevention and TB Elimination, and security and computer staff in other Centers and Offices within CDC, and on reviews by state and local surveillance programs.

This document requires each cooperative agreement grantee to designate an Overall Responsible Party (ORP). The ORP will have the 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 should be a high-ranking public health official. This official should have the authority to make decisions about surveillance operations that may affect programs outside of HIV/AIDS surveillance. The ORP is responsible for determining how surveillance information will be protected when it is collected, stored, analyzed, released, and dispositioned.

Although there are many sources of surveillance information (e.g., medical charts, insurance forms, behavioral surveys, and service organizations), the authority of this document is limited to data collected for HIV/AIDS surveillance. Data in the HIV/AIDS surveillance system are to be held under the highest scrutiny and require the most stringent protections, regardless of the level of security of the source data or of non-HIV surveillance data. A breach of confidentiality anywhere in this system could affect surveillance operations nationwide. All references in these guidelines to surveillance information and data should be understood to refer only to HIV/AIDS-related surveillance. These security guidelines may serve as a model for other programs to emulate when reviewing or upgrading security protocols that are specific to their overall procedures and mission. For programs that integrate HIV and other disease surveillance, all data should be protected equally in compliance with these guidelines.

This document is intended to assist programs in providing aggregate data for maximum public health utility with minimum risk of disclosure of individual-level data. Given the advances in information technology, as well as changes in surveillance practices since the previous update in 1998, the guidelines are being updated to provide project areas with guidance reflecting those changes. CDC will continue to assist states as they adapt their policies and procedures to comply with evolving requirements and standards.

Existing Protections

HIV/AIDS surveillance is the joint responsibility of many participants in the health care system. Among the participants are state and local health department surveillance programs; public and private institutions providing clinical, counseling, and laboratory services; individual health care providers; persons at risk for HIV infection; and persons

with HIV or AIDS. The ability of state and local surveillance programs to collect, store, use, and transmit sensitive HIV/AIDS case information in a secure and confidential manner is central to the program's acceptability and success. The importance of data security has been a long-established component of these guidelines. Various federal and state statutes, regulations, and case law provide legal protection of HIV/AIDS surveillance information. Among these safeguards are a right to informational privacy under the Fifth and Fourteenth Amendments to the Constitution, and federal assurance of confidentiality (under § 308(d) of the Public Health Service Act and various state and local protections).

The dynamic nature of information technology is a critical consideration in developing security policies and procedures that will be used to meet the requirements and standards described in these guidelines. The HIV/AIDS surveillance system was created before the development of technologies such as laptops, portable external storage devices, and the Internet, all of which can be potential sources for security breaches. Now, all state and local health departments should routinely assess the changing world of computer technology and adjust security policies and procedures to protect against potential new risks. CDC is available to provide technical consultation on technology and security issues.

Purpose of Guidelines

Scope

The security standards presented here are intended to apply to local, state, and territorial staff and contractors funded through CDC to perform HIV/AIDS surveillance activities and at all sites where an HIV/AIDS reporting system is maintained.

Although designed for HIV/AIDS surveillance activities, these security standards may serve as a model for other programs to use in reviewing or upgrading security protocols that are appropriate for their overall procedures and mission. Although health care providers who are the source of surveillance information are not under an obligation to follow these security standards, local and state surveillance staff may nevertheless suggest portions of these standards to providers to foster a shared stewardship of sensitive information by promoting security and confidentiality protections in provider settings.

Providers concerned with the Health Insurance Portability and Accountability Act (HIPAA) may use these guidelines as a foundation for their HIPAA compliance policies; however, these guidelines are not a guarantee of HIPAA compliance within a provider setting. Providers need to use their own resources to evaluate their everyday compliance. HIV/AIDS surveillance programs should remind providers that HIPAA permits public health reporting requirements and that providers are still subject to relevant laws, regulations, and public health practices, as described in the MMWR available from http://www.cdc.gov/mmwr/PDF/wk/mm52SU01.pdf. Surveillance staff can also find answers to many frequently asked questions regarding HIPAA and public health at the Office of Civil Rights Web site at http://www.hhs.gov/ocr/hipaa.

The HIV/AIDS surveillance system was not designed for case management purposes, and CDC does not provide surveillance funds to states to support case management or referral services. However, some states and territories have chosen to use information from

individual case reports to offer voluntary referrals to prevention and care services, including partner notification assistance. The confidentiality and security issues associated with the provision of those services are outside the scope of this document. When considering such releases of individual-level data from the HIV/AIDS reporting system to other HIV prevention and care programs, state and local health officials should have mechanisms in place to inform and receive input from community members, such as prevention planning groups. Officials must require that recipients of surveillance information have well-defined public health objectives and that they have compared the effectiveness of using confidential surveillance data in meeting those objectives with other strategies. Furthermore, recipients of surveillance information must be subject to the same training and penalties for unauthorized disclosure as surveillance staff.

Data collected by sites through surveillance activities and reported to CDC originate in health care provider, institutional, and laboratory settings. From these sources, confidential information on persons with HIV/AIDS may be obtained in accordance with state law, regulation, or rule. The convenience of having HIV/AIDS surveillance data should not be considered a justification for using it for nonpublic health purposes in preference to more appropriate sources of individual-level data. State and local HIV/AIDS surveillance programs must develop data release policies that include restrictions on the use of surveillance data for nonpublic health purposes. Refer to the Policies section of this document for policy requirements.

A separate set of protections covers HIV/AIDS surveillance information and data maintained at CDC. To protect the confidentiality of persons reported with HIV/AIDS, local and state surveillance program staff do not send names and other specific identifying information to CDC. Additional protections are provided by exemptions to the Freedom of Information Act of 1966 (specifically U.S.C. 552(b)[6]) and by the Privacy Act of 1974. Most importantly, the Assurance of Confidentiality authorized by 308(d) of the Public Health Service Act enables CDC to withhold disclosure of any HIV/AIDS surveillance-related information. A copy of the Assurance of Confidentiality statement can be found in Attachment D. Any HIV/AIDS-related human subject research (as distinguished from routine HIV/AIDS surveillance) conducted or supported by CDC must be approved by an Institutional Review Board (IRB). A key condition of IRB approval is that provisions must be in place to protect the privacy of subjects and to maintain the confidentiality of data.

Requirements and Standards

The requirements and standards in this document are designed for state and local HIV/AIDS surveillance agencies to use as both a guide to the surveillance staff and a basis for corrective action when conduct falls below the required minimum standards as stated in the various requirements. These guidelines also define the standard of conduct that the public should expect of HIV/AIDS surveillance staff in protecting private and sensitive information. Attending to the details of good public health practice creates a professional environment for surveillance staff. Good public health practice dictates that HIV/AIDS surveillance data are used only for the purposes for which they were collected.

This document is divided into security-related topics. Each topic contains both program requirements and discussions that serve to either explain the requirement or offer security considerations that will help comply with the requirement.

Program requirements are mandatory, and the ORP will certify them annually. See Requirement 10. Each requirement states the minimum standard that surveillance staff must achieve. Falling below this standard could result in corrective action. These standards do not prescribe the penalty that should result from a violation of a program requirement. The ORP, considering the nature of the offense, the surrounding circumstances, local policy, and state law, should determine those decisions. Discipline may range from an employee reprimand to criminal charges.

Additional security considerations, unlike the program requirements, are aspirational and represent the objectives that each member of the surveillance staff should strive to achieve. They comprise a body of principles that surveillance staff can rely upon for guidance in many specific situations. For a list of additional security considerations, refer to Attachment A: Additional Laptop Security Considerations and Attachment B: Additional Security and Policy Considerations.

Guiding Principles

The five guiding principles listed next are the backbone upon which all program requirements and security considerations are derived. The applicable guiding principle is referenced at the end of each program requirement (e.g., GP-1), so a reader can determine the principle that is being addressed by the requirement.

Guiding Principle 1

HIV/AIDS surveillance information and data will be maintained in a physically secure environment. Refer to sections Physical Security and Removable and External Storage Devices.

Guiding Principle 2

Electronic HIV/AIDS surveillance data will be held in a technically secure environment, with the number of data repositories and individuals permitted access kept to a minimum. Operational security procedures will be implemented and documented to minimize the number of staff that have access to personal identifiers and to minimize the number of locations where personal identifiers are stored. Refer to sections Policies, Training, Data Security, Access Control, Laptops and Portable Devices, and Removable and External Storage Devices.

Guiding Principle 3

Individual surveillance staff members and persons authorized to access case-specific information will be responsible for protecting confidential HIV/AIDS surveillance information and data. Refer to sections Responsibilities, Training, and Removable and External Storage Devices.

Guiding Principle 4

Security breaches of HIV/AIDS surveillance information or data will be investigated thoroughly, and sanctions imposed as appropriate. Refer to section Security Breaches.

Guiding Principle 5

Security practices and written policies will be continuously reviewed, assessed, and as necessary, changed to improve the protection of confidential HIV/AIDS surveillance information and data. Refer to sections Policies and Security and Confidentiality Program Requirement Checklist.

Also included in the document are a series of attachments that provide specific information on various topics that would be either too detailed or inappropriate in the body of this document. The following eight documents are attached:

Attachment A: Additional Laptop Security Considerations

Attachment B: Additional Security and Policy Considerations

Attachment C: Federal Encryption Standards

Attachment D: CDC Assurance of Confidentiality

Attachment E: Sample Employee Oath - Texas

Sample Employee Oath - Seattle/King County

Sample Employee Oath - Louisiana

Attachment F: Glossary of Surveillance and Technical Terms

Attachment G: Using HIV Surveillance Data to Document Need and Initiate Referrals

Attachment H: Security and Confidentiality Program Requirement Checklist

Policies

Requirement 1 Policies must be in writing. (GP-2)

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

The name of the individual who is designated as the ORP, rather than an organizational position, must be provided to CDC annually. The rationale is to increase accountability and help ensure that the individual knows his/her responsibilities as ORP.

Requirement 3 A policy must describe methods for the review of security practices for HIV/AIDS surveillance data. Included in the policy should be a requirement for an ongoing review of evolving technology to ensure that data remain secure. (GP-5)

As part of a review and quality improvement procedure, sites may consider a self-administered procedure by using the *Security and Confidentiality Program Requirement Checklist* shown in Attachment H (or a similar form tailored for local use) and refer to the log of breaches.

Requirement 4 Access to and uses of surveillance information or data must be defined in a data release policy. (GP-2)

Requirement 5 A policy must incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying. (GP-2)

Data release policies outline the types of data that can be released and who is authorized to receive the data. For example, with regard to matching HIV/AIDS cases to cases in other data stores (e.g., TB, STD, or vital statistics), the policy should specify what the purpose is, how this is done, who performs the matching, what results are released, how the results should be stored, and who receives the results.

This policy establishes the rules to be implemented to ensure that information is allowed to flow within the information system and across system boundaries only as authorized. Data release, by definition, suggests that information about an HIV-infected individual is available for distribution. A data release policy has to balance the inherent purpose of HIV/AIDS surveillance data with the confidentiality of any HIV-infected individual reported for surveillance purposes. Therefore, any HIV/AIDS surveillance data release policy must be written with two questions in mind. First, which data elements can be released about any case patient that would not identify the individual if pieced together? Second, what purposes are consistent with the reasons for which the data were originally collected?

With regard to the first question, certain information containing patient identifying data elements (including elements such as patient's name, address, and social security number) may never be released for public distribution. Care must also be taken to ensure that information released cannot be linked with other databases containing additional information that can be used to identify someone. However, in developing a data release policy, state and local HIV/AIDS surveillance programs should be aware that several data elements that are not inherently identifying could be linked together to identify an individual. For example, when releasing data on a community with relatively few members of a racial/ethnic group (e.g., Asian/Pacific Islanders or American Indians/Alaska Natives), a risk factor group (e.g., persons with hemophilia), or an age group (e.g., >50 years old or specifying the date of birth or death), surveillance staff should be careful that release of aggregate data on the distribution of HIV-infected individuals by these categories could not suggest the identity of an individual. Time periods also need to be considered when developing a data release policy. Output from cases reported cumulatively (since 1981) better hides any individual's identity than output from cases reported within the past 12 months. Therefore, care should be taken in deciding how both the numerator and the denominator are defined when developing a data release policy.

Traditionally, surveillance data are released as aggregated data. As a rule, CDC will not release national aggregated data in tables when the number of records reflected in a cell falls below a minimum size, depending on sensitivity of the data. Some states have similar cell size restrictions. Most states consider the denominator size of the population under analysis and may release small cells under certain circumstances. However, as described previously, even cell size limitations could allow for inferential identification of an individual. Care should also be taken in graphic presentation of data. For example, geographic information systems (GIS) allow for relatively accurate dot mapping of observations. Care must be taken that graphic (like numeric) presentation of data cannot permit the identification of any individual by noting pinpoint observations of HIV cases at, for example, the county, ZIP code, or census tract level. Other considerations in developing data release policies include the need for state surveillance programs to assure that their data release policies are consistent with state confidentiality laws, and to include clear definitions of terms used in the data release policy (e.g., personal identifier, population size, and time period). For a complete discussion covering this issue, refer to the chapter on <*Data Analysis and Dissemination*>.

The second issue that should guide the development of a data release policy is to consider the purpose for which the data were originally collected. To be consistent with the federal Assurance of Confidentiality under which CDC collects HIV data and the purpose for which CDC provides support to states to conduct surveillance, no HIV surveillance information that could be used to identify an individual should be available to anyone for nonpublic health purposes. Examples include the release of individual-level data to the public; to parties involved in civil, criminal, or administrative litigation; for commercial purposes; or to nonpublic health agencies of the federal, state, or local government. Surveillance data are collected to monitor trends in the epidemic on a population-based level. However, some state and local surveillance programs have chosen to share individual case reports with prevention and care programs to initiate referrals to services. Additionally, some surveillance programs use surveillance data to initiate follow-up for supplemental public health research. Programs that choose to establish these linkages should do so without compromising the quality or security of the surveillance system and should establish principles and procedures for such practices in collaboration with providers and community partners. Programs that receive surveillance information should be subject to the same penalties for unauthorized disclosure and must maintain the data in a secure and confidential manner consistent with CDC surveillance guidelines. Additionally, activities deemed to be research should get appropriate human subjects approvals consistent with state and local health department procedures. A discussion on using HIV surveillance data to initiate referrals to prevention or treatment services is available in the document *Integrating HIV and AIDS Surveillance: A Resource Manual for Surveillance Coordinators - Toolkit 5, Using HIV Surveillance Data to Document Need and Initiate Referrals*, found in Attachment G. Several other CDC resources and guidance documents are available online to inform local discussions, including *HIV Partner Counseling and Referral Services: Guidance*, *HIV Prevention Case Management: Guidance*, resources on evaluation of HIV prevention programs, and more at http://www.cdc.gov/hiv/pubs/guidelines.htm. The HIV Incidence and

Case Surveillance Branch is currently working on ethical guidelines for the use of public health data for HIV/AIDS. Please contact your HIV surveillance program consultant for additional information on these guidelines.

Requirement 6 Policies must be readily accessible by any staff having access to confidential surveillance information or data at the central level and, if applicable, at noncentral sites. (GP-2)

As security questions arise in the course of surveillance activities, staff must have ready access to the written policies. In most circumstances, having a copy of the written policies located within the surveillance unit would satisfy this requirement. Computer access to an electronic version of the policies also may be acceptable. The key is for staff to have quick access to policies as security and confidentiality questions arise.

Requirement 7 A policy must define the roles for all persons who are authorized to access what specific information and, for those staff outside the surveillance unit, what standard procedures or methods will be used when access is determined to be necessary. (GP-2)

Requirement 8 All authorized staff must annually sign a confidentiality statement. Newly hired staff must sign a confidentiality statement before access to surveillance data is authorized. The new employee or newly authorized staff must show the signed confidentiality statement to the grantor of passwords and keys before passwords and keys are assigned. This statement must indicate that the employee understands and agrees that surveillance information or data will not be released to any individual not granted access by the ORP. The original statement must be held in the employee's personnel file and a copy given to the employee. (GP-2)

The policy should establish rules to ensure that only designated individuals, under specified conditions, can

- Access the information system (network logon, establish connection),
- Activate specific system commands (execute specific programs and procedures; create, view, or modify specific objects, programs, information system parameters). The policy should include provisions for periodic review of access authorizations. Note that CDC's HIV/AIDS Reporting System does not have the ability within the application to establish access times.

The policy could limit access to sensitive data to specified hours and days of the week. It should also state types of access needed, which could be linked to roles defined for those with access. For example, epidemiologists may have access to data across programs that do not include identifiers.

Additionally, the policy should cover restrictions on access to the public Internet or e-mail applications while accessing surveillance information. Accidental transmission of data through either of these systems can be avoided if they are never accessed simultaneously. Similarly, intruders can be stymied in attempts to access information if it is not available while that connection is open.

The policy should establish rules that ensure that group authenticators (administrators, super users, etc.) are used for information system access only when explicitly authorized and in conjunction with other authenticators as appropriate. The policy should express similar rules for individual users to ensure that access to identifiable data is allowed only when explicitly authorized and in conjunction with other authenticators as appropriate. The policy should document the process for assigning authorization and identify those with approval authority. Information technology (IT) authorities granting access must obtain approval from the ORP or designee before adding users, and they should maintain logs documenting authorized users. The ORP or a designee should periodically review user logs.

Requirement 9 A policy must outline procedures for handling incoming mail to and outgoing mail from the surveillance unit. The amount and sensitivity of information contained in any one piece of mail must be kept to a minimum. (GP-2)

The U.S. Mail and other carrier services are commonly used for the movement of paper copies of information. There are many ways that project areas can protect the confidentiality of an HIV-infected individual when using the mail. For example, when surveillance staff and providers are mailing information (e.g., case report forms) to the central office, the policy could require that names and corresponding patient numbers be sent in one envelope, while the remaining information referenced by the corresponding patient number is sent in another envelope. In addition, the terms 'HIV' or 'AIDS' should not necessarily be included in either the mailing address or the return address. Mailing labels or pre-addressed, stamped envelopes may be supplied to field staff and providers to encourage this practice and to ensure the use of the correct mailing address. Whenever confidential information is mailed, double envelopes should be used, with the inside envelope clearly marked as confidential.

Because of the potential number of entries on a given paper copy line list, programs must exercise extreme caution if they find it necessary to mail a paper list. Procedures for mailing lists, including the amount and type of information permitted in any one mailing, must be clearly outlined in the local policy. Two methods that surveillance programs currently employ to minimize risk when using the mail are (1) to generate lists containing names without references to HIV or AIDS or (2) to remove the names from the list and mail them separately from the other sensitive information.

Responsibilities

Requirement 10 In compliance with CDC's cooperative agreement requirement, the ORP must certify annually that all program requirements are met. (GP-2)

Requirement 11 Each member of the surveillance staff and all persons described in this document who are authorized to access case-specific information must be knowledgeable about the organization's information security policies and procedures. (GP-3)

Requirement 12 All staff who are authorized to access surveillance data must be responsible for challenging those who are not authorized to access surveillance data. (GP-3)

Many programs consider the area of personal responsibility as a potential area of concern because the actions of individuals within a surveillance system are much more difficult to proscribe than operational practices. This area represents one of the most important aspects of holding data in a secure and confidential fashion, but the development of objective criteria for assessing the degree of personal responsibility in individual staff members may be difficult.

The program requirements in this area may be evaluated objectively by using a series of questions supervisors pose during the annual review of security measures with staff. Input from staff can be obtained through such questions as these:

- How often do you find the need to reference local or CDC security policies or standards?
- Do you know who (by job position or name) should have access to the secure surveillance area? How would you approach someone who was entering the secured room whom you believe was not authorized access? Have you had any occasion to challenge such a person?
- To whom should security irregularities be reported? What are some examples of what would constitute an irregularity? What irregularities would not need to be reported, if any?
- Who else needs access to your computer for any reason? For example, do family members or other staff members ever need to use your workstation? Do you ever need to lend your key to a secured area to another member of the health department staff for after-hours access to the building? Who else knows your computer passwords?

Requirement 13 All staff who are authorized to access surveillance data must be individually responsible for protecting their own workstation, laptop, or other devices associated with confidential surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Staff must take care not to infect surveillance software with computer viruses and not to damage hardware through exposure to extreme heat or cold. (GP-3)

Surveillance staff should avoid situations that might allow unauthorized persons to overhear or see confidential surveillance information. For example, staff should never discuss confidential surveillance information in the presence of persons who are not authorized to access the data. Staff working with personal identifiers should have a

workspace that does not allow phone conversations to be overheard or paperwork and computer monitors to be observed by unauthorized personnel. Ideally, only staff with similar roles and authorizations would be permitted in a secure, restricted area.

Training

Requirement 14 Every individual with access to surveillance data must attend security training annually. The date of training must be documented in the employee's personnel file. IT staff and contractors who require access to data must undergo the same training as surveillance staff and sign the same agreements. This requirement applies to any staff with access to servers, workstations, backup devices, etc. (GP-3)

Security training is required for all new staff and must be repeated annually thereafter, but the nature of this training may vary based on local circumstances. For example, in areas of low HIV prevalence where one surveillance person is on staff, if that person leaves before training a replacement, the policy should indicate that training for data security and confidentiality may be obtained in a neighboring state. In other areas, new staff may be trained by the surveillance coordinator one-on-one. In this instance, the policy should document what types of information must be covered in such a session, and provisions should be made to document that training was completed. In areas of high HIV prevalence with larger numbers of staff, periodic group training sessions may be more appropriate.

Physical Security

Requirement 15 All physical locations containing electronic or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access. Workspace for individuals with access to surveillance information must also be within a secure locked area. (GP-1)

Requirement 16 Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room. (GP-1)

Requirement 17 Each member of the surveillance staff must shred documents containing confidential information before disposing of them. Shredders should be of commercial quality with a crosscutting feature. (GP-3)

Maximum security practice dictates that HIV/AIDS surveillance data be maintained on a dedicated file server at only one site in each project area where layers of security protections can be provided in a cost-effective manner. This would obviate the need to duplicate expensive security measures at multiple locations throughout the state. Remote sites that need access to the central surveillance server for surveillance activities could access the server through a secured method (e.g., virtual private network [VPN], or authentication server) set up for authorized users. Analysis databases available to all intrastate jurisdictions would allow the data to be used for analysis and program planning at the local level. As resources permit, CDC technical

and financial assistance may be available to assist states in moving to a more centralized surveillance operation. See section Central, Decentral, and Remote Access for details.

CDC recognizes that, for some surveillance programs, it may not be possible at this time to limit the entry of HIV/AIDS data into a reporting system located at a single site. Based on local health department policies and organization, some states have decided to maintain the reporting system in more than one site. If this is the case, every additional reporting system site in the state must meet the same minimum security measures outlined in all of the program requirements.

Because the surveillance system can potentially identify any number of persons with HIV/AIDS within a state (or local jurisdiction if surveillance is decentralized), particular attention to the security of surveillance information is critical. CDC's requirement to house the surveillance information in a locked room is long standing and has been part of the surveillance guidance for many years. Jurisdictions use various security methods to hold HIV/AIDS case data stores, but the minimum security standard is to enclose the surveillance information inside a locked room regardless of the method used. Whether the reporting system resides on a server or workstation, the computer containing the electronic surveillance data must be enclosed inside a locked room. Only authorized surveillance personnel should have access to the locked room. However, depending on the numbers of HIV/AIDS cases reported, the size and role of the surveillance staff, community interest, and health department resources, the ORP may decide that other authorized health department staff may need to work inside the surveillance room.

If the surveillance data reside on a server inside a locked room and not on the hard drive of any individual workstation within the department, the individual workstation (when logged off the network) does not pose a great security risk and would not necessarily have to be located behind a locked door to meet the minimum standard. However, most health departments using Local Area Network (LAN) systems to maintain surveillance data require both the workstation and the server to be located in rooms with doors that lock. LAN accounts with access to identifying information in the reporting system should be limited only to the workstations of those authorized. LAN accounts also should be limited by time of day. See Requirement 7.

The use of cubicles in many office buildings can also present a challenge to creation of a secure area. Cubicles with low walls make it difficult, even within a secure area, to have a telephone conversation without others hearing parts of the conversation. Where necessary, higher cubicle walls with additional soundproofing can be used. When cubicles are part of the office structure, cubicles where sensitive information is viewed, discussed, or is otherwise present should be separated from cubicles where staff without access to this information are located.

When electronic surveillance data with personal identifiers are stored outside of a physically secure area (i.e., a locked room with limited access), or if limited local resources require that surveillance data with personal identifiers stored on a LAN be accessible to nonsurveillance staff, real-time encryption software must be employed. The additional encryption software is designed to keep identifying information

encrypted. Should an unauthorized individual gain access to the surveillance database, unencrypted identifying information cannot be viewed. Encryption software that meets federal standards must be used before data are transmitted to CDC. See Attachment C: Federal Encryption Standards and section Sending Data to CDC for details. Encryption requirements would also apply to backup storage media, which are frequently located off-site and could be managed by an outside vendor.

Paper copy data stores must be maintained in a locked cabinet and inside a locked room. If an area chooses to no longer maintain paper copies in locked file cabinets inside a locked room (e.g., because of age or volume), the program should destroy the completed forms after ensuring the data are entered into the reporting system and after they are no longer needed for follow-up. Before destroying the forms, a site may opt to digitally scan forms for future reference. Digitized forms should be secured the same as any other surveillance data. Requirement 15 does not apply to subsets of case report forms, such as those that a surveillance staff member may hold in the course of an investigation, but does apply to paper copy line lists or logbooks that list a large number of reported cases by name in any one jurisdiction. Even if appropriate space is available to properly store all surveillance forms, program staff should consider developing a records retention policy that would describe the record retention and the scheduling of records for destruction after a designated period. Older records offer only limited value, but continue to pose a security risk. Sites should carefully weigh the benefits and risks of retaining any paper copies of case report forms. Such a decision should be predicated on adherence to these security standards, state regulations, and local practice. Once a decision has been made to destroy a case report form, line list, notes, or any other related paper surveillance document, the document must be destroyed in accordance with Requirement 17.

Requirement 18 Rooms containing surveillance data must not be easily accessible by window. (GP-1)

Window access, for the purposes of this document, is defined as having a window that could allow easy entry into a room containing surveillance data. This does not mean that the room cannot have windows; rather, windows need to be secure. If windows cannot be made secure, surveillance data must be moved to a secure location to meet this requirement.

A window with access, for example, may be one that opens and is on the first floor. To secure such a window, a permanent seal or a security alarm may be installed on the window itself. Even if the window does not open, program managers may decide to include extra precautions if, for example, the building does not have security patrols or if the building or neighboring buildings have had breaches. If a project area has a concern about a current or planned physical location, staff can request advice from CDC.

Data Security

For the purposes of this document, a remote site is defined as a site that remotely connects to and accesses a centralized electronic database to enter and store surveillance data even though paper forms may be stored locally. The central database is located in a different

physical location than the remote site and usually in a different city. A satellite location is defined as a site that collects and electronically enters surveillance data in a local database and then sends the electronic data file to a central location. If remote and satellite sites maintain case report forms or other surveillance information with personal identifiers, the central location should not be maintaining duplicate copies of the case report forms. Surveillance staff should discourage providers from maintaining duplicate copies of HIV/AIDS case reports after they have been reported to the health department.

The statewide HIV/AIDS case database should be housed in only one location (excluding electronic backups and replication for disaster recovery); however, as states with multiple database locations move to more centralized operations, the number of satellite locations within a state should be kept to a minimum, thereby keeping the data collection and storage as centralized as possible. If the system is decentralized, each remote and satellite site should maintain only cases within that site's jurisdiction, and must meet the same physical security requirements discussed in section Physical Security.

If, after discussing a records retention schedule, program staff decide to retain the hard copy case report form even after the record is entered into the reporting system, they should consider removing or striking out the name on the report before storage. The state patient number would still provide linkage, when necessary, to the name in the reporting system while improving record security. This practice would decrease (1) the number of places where names are stored, (2) the amount of time they are held, and (3) the number of persons who may have access to them in the future.

Security software that controls the storage, removal, and use of data maintained in the reporting system should be in place at all locations where the electronic surveillance data are maintained. Security software may include such protections as user identifications, passwords, boot protection, encryption algorithms, and digital signatures. Additionally, an area may maintain names outside of the reporting system and use a state ID number to link name and surveillance information when needed.

Data Movement

Requirement 19 Surveillance information must have personal identifiers removed (an analysis dataset) if taken out of the secured area or accessed from an unsecured area. (GP-1)

Requirement 20 An analysis dataset must be held securely by using protective software (i.e., software that controls the storage, removal, and use of the data). (GP-1)

Requirement 21 Data transfers and methods for data collection must be approved by the ORP and incorporate the use of access controls. Confidential surveillance data or information must be encrypted before electronic transfer. Ancillary databases or other electronic files used by surveillance also need to be encrypted when not in use. (GP-1)

Electronic files stored for use by authorized surveillance staff should be encrypted until they are actually needed. If these files are needed outside of the secure area, real-time encryption or an equivalent method of protection is required.

This requirement also applies in those situations where surveillance data are obtained electronically from external sources (clinical data management systems and laboratories) or as part of a separate health department data collection system (Careware for example). Extracts from those systems need to be protected as if they were extracts from the surveillance data system. Additionally, those systems within the health department need to be held to the same standards as the HIV/AIDS surveillance systems. External agencies are to be encouraged to review their procedures, and approved data transfer methods need to be used.

Requirement 22 When case-specific information is electronically transmitted, any transmission that does not incorporate the use of an encryption package meeting the Advanced Encryption Standard (AES) encryption standards and approved by the ORP must not contain identifying information or use terms easily associated with HIV/AIDS. The terms HIV or AIDS, or specific behavioral information must not appear anywhere in the context of the communication, including the sender and/or recipient address and label. (GP-2)

The intent of this requirement is to eliminate the possibility that a third party may identify a person as being a member of an HIV risk factor group or HIV infected. For example, when trying to locate an HIV-infected person during an NIR (No Identified Risk) investigation or interview, do not send letters or leave business cards or voice messages at the person's residence that include any terminology that could be associated with HIV, AIDS, or the health department. These precautions need to be taken in case a family member or friend discovers the letter or card or hears the voice message. Similarly, if a third party calls the telephone number listed on a card or letter, that party should not be able to determine by a phone greeting that it is an HIV/AIDS surveillance unit (or the health department); nor should a third party be able to obtain that information by pretending to be the case patient. This may require the use of some confirmation mechanism to assure that the person calling really is the case patient and not someone pretending to be that person to discover confidential information. For additional information on confidential interview techniques, you may request CDC interview guidelines by contacting your CDC program consultant.

If secure fax or encrypted e-mail transmissions are used at all (although CDC strongly discourages their use), care must be taken to avoid linking HIV or risk factor status with identifiable information about a person. This may include ensuring that the terms HIV or AIDS do not appear in the fine print at the very top of a fax indicating who sent it and that these terms do not appear in more obvious locations in the letterhead and body of the fax. Other important steps include thinking about who else besides the intended recipient may have access to faxes on the receiving end and the possibility of misdialing the fax number or using the incorrect e-mail address.

Requirement 23 When identifying information is taken from secured areas and included on line lists or supporting notes, in either electronic or hard copy format, these documents must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any information that could easily be associated with HIV or AIDS. (GP-1)

One purpose of this requirement is to make it difficult to link an individual's name on a line list with HIV/AIDS should that line list fall into the hands of an unauthorized person. Terms that could be associated with HIV/AIDS include CD4 count or opportunistic infection (OI). Programs should consider using less recognizable terms, codes, or abbreviations such as T-lymphocyte count or OI. In some circumstances, just the word "count" may suffice. While risk factor information (e.g., injection drug use or sexual orientation) may not necessarily be associated with HIV/AIDS, it nevertheless is highly sensitive. Wherever possible, risk factor categories must be coded to help minimize the possibility of a breach. A coding scheme for transmission category is already built into the reporting system and should be used when there is a need to generate line lists with risk factor categories. When surveillance staff write notes, they should make it a habit to use these risk factor codes. For example, instead of using the phrase injection drug user or the readily decipherable abbreviation IDU, a code could be substituted.

This requirement applies to information or data taken from secure areas. It does not refer to data collected from the field and taken to secure areas. While coding of terms associated with HIV/AIDS in the field is encouraged, there may be occasions when it cannot be done, for example, when uncoded terminology must be abstracted from a medical chart on a No Identified Risk case during the course of an investigation.

Requirement 24 Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the surveillance coordinator. (GP-1)

Under exceptional circumstances, HIV/AIDS surveillance information with personal identifiers may be taken to private residences without approval if an unforeseen situation arises that would make returning to the surveillance office impossible or unsafe. For example, if a worker carrying sensitive information were caught in a sudden heavy snowstorm, driving home instead of returning to the office would be permissible provided the worker's supervisor is notified (or an attempt was made to notify the supervisor) of the need to return home with the sensitive information. Precautions should be taken at the worker's home to protect the information under such circumstances. All completed, or partially completed, paper case report forms should be transported in a locked satchel or briefcase.

Managing field time effectively can be accomplished by using a variety of creative tactics. Field visits should be scheduled in the most efficient way possible. One option is to assign provider sites to workers by geographic area. For example, all providers in the east sector could be covered by the same worker to minimize travel time between sites. Another option might be to schedule visits so that sites located far from the

office receive visits early in the day with staff working their way back to the office by the end of the day. A flextime schedule is another option that a site may wish to consider.

If returning to the secured area creates significant inefficiencies in case surveillance investigations, alternative methods of securing sensitive surveillance information could be considered when developing the policy that satisfies this requirement. Investigators could incorporate the use of pre-addressed, stamped envelopes and drop completed case report forms in the mail before returning home for the day. Tampering with the mail is a felony, and case reports are considered better protected in the mail than at a private residence. This possibility should be accounted for when developing the mail policy discussed in Requirement 9.

Some areas do not complete case report forms on-site, but take notes using shorthand that is not easily translated and does not contain HIV-related terms. Notes such as these could be stored in less secure areas because someone seeing the notes would not understand their meaning. When this method is used, blank case report forms or other HIV-related materials should not be stored at the same location as the notes. Staff using this technique may carry the notes around discreetly (e.g., in a purse or notebook) and then complete official forms when they return to the surveillance office. Other methods to disguise the data, de-identify it, or separate sensitive variables from it could be used to eliminate the need to return to the office at the close of business (i.e., if personal identifiers are removed using approved methods, the information is less sensitive and may be secured off-site). Whatever methods are used, the approved method must be described in the local security policy.

Requirement 25 Prior approval must be obtained from the surveillance coordinator when planned business travel precludes the return of surveillance information with personal identifiers to the secured area by the close of business on the same day. (GP-1)

Policies and procedures for gaining prior approval for not returning surveillance information with personal identifiers to the secured area at the close of each business should be implemented. Refer to the discussion following Requirement 24 for additional considerations.

Sending Data to CDC

CDC's policy requires encryption when any moderately or highly sensitive files, any moderately or highly critical information, or any limited access/proprietary information is to be transmitted to or from CDC either electronically or physically. All data that meet these criteria must be encrypted using the Advanced Encryption Standard (AES). See Attachment C for details describing federal encryption standards. Currently, CDC requires that this category of electronic data be sent via its Secure Data Network (SDN). Future considerations may include sending data using the Public Health Information Network Messaging System (PHIN MS). The SDN uses digital certificate technology to create a Secure Sockets Layer (SSL) or encrypted tunnel through which data are transmitted. The SSL is broken once the client browser loses connectivity with the CDC Web server, which is located outside of its firewall.

To protect sensitive data once the SSL is broken and as they move between various CDC servers, CDC requires that sensitive data be encrypted with a product that meets federal standards. To support that requirement, CDC can provide users with a free CDC-produced, Java-based software called SEAL. Some CDC programs will also accept files encrypted with commercially available products. A site must coordinate efforts with CDC if the site wishes to use a commercially available encryption product. Any commercially available product selected must meet federal AES standards.

Note: The HIV/AIDS Reporting System (HARS) transfer files are output with a 40-bit encryption algorithm that does not meet the standards. Therefore, HARS files must be encrypted before being sent to CDC via the SDN. The e-HARS transfer files are output with a 1024-bit SEAL encrypted algorithm that does meet the standards, and, therefore, no additional encryption will be necessary before sending to CDC.

Transferring Data between Sites

Many sites have a need to move data within a state or between states. If these data meet the criteria described in the previous topic, Sending Data to CDC, CDC strongly recommends that these data be encrypted. CDC has no mechanism in place to support non-CDC transfers. The sending and receiving sites must agree on the product that will be used for that purpose and identify the method of transfer. CDC will provide, upon request, the full version of the SEAL software; however, SEAL is a Java-based application that is executed within a DOS shell. SEAL does not have a graphical user interface (GUI). Many inexpensive, commercially available, easier to use, object-oriented software products are available for purchase. Additionally, a site may wish to consider the PHIN MS for point-to-point encryption and movement of data. For more details regarding PHIN MS, refer to the Web site http://www.cdc.gov/phin/messaging.

Access Control

Local Access

Requirement 26 Access to any surveillance information containing names for research purposes (that is, for other than routine surveillance purposes) must be contingent on a demonstrated need for the names, an Institutional Review Board (IRB) approval, and the signing of a confidentiality statement regarding rules of access and final disposition of the information. Access to surveillance data or information without names for research purposes beyond routine surveillance may still require IRB approval depending on the numbers and types of variables requested in accordance with local data release policies. (GP-1)

Most analyses of HIV/AIDS surveillance data do not require IRB approval; in fact, most such analyses do not require the inclusion of identifying information in the data sets. Occasionally, investigators from other health department units or academia want to conduct supplemental studies using reported case patients as their study population. Additionally, clinic-based researchers may want to obtain additional information on their patients. In these cases, the researcher should submit a request for the data set to

the HIV/AIDS surveillance coordinator. The surveillance coordinator should then refer to the local data release policy to determine if any of these types of data sets can be released. Data containing patients' names are not normally released for research purposes; further, the data release policy should anticipate that even data not containing names could be used to breach an individual's confidentiality if data sets are created or can be created that could indirectly identify any individual (e.g., a data set of all Asian hemophiliacs with AIDS in a county with a low Asian population and low morbidity).

Under certain circumstances and in accordance with local data release policies, the surveillance coordinator should refer the researcher to the Chair of the IRB. If the Chair determines that an IRB should be convened, both the researcher and surveillance coordinator must abide by the ruling. The IRB may approve the release of an analysis data set. Before a researcher obtains access to a data set, the surveillance coordinator must obtain a signed statement from the researcher certifying that he or she will comply with standards outlined in the local security policy. Signing this statement should indicate that the researcher (1) understands the penalties for unauthorized disclosure, (2) assures that the data will be stored in a secured area, and (3) agrees to sanitize or destroy any diskettes or other storage devices that contained the data set when the research project is completed. If the researcher is a member of the HIV/AIDS surveillance unit and already has a signed confidentiality statement on file, there is no need to sign an additional statement.

Under a signed assurance of confidentiality (see Attachment D), the HIV/AIDS surveillance information received by CDC that permits the identification of any individual is collected with a guarantee that it (1) will be held in strict confidence, (2) will be used only for purposes stated in the assurance, and (3) will not otherwise be disclosed or released without the consent of the individual in accordance with sections 306 and 308(d) of the Public Health Service Act.

Analysis databases or data sets that are released to individuals who work outside the secured area must be held securely until the data are approved for release. For example, health department epidemiologists or statisticians who do not work in the secured area often use analysis databases for routine analysis. The computers used in these circumstances must have protective software (e.g., user ID and password protection) to maintain data securely. Other robust authentication methods also may be used since the examples described are only the minimum required. Encryption software is not required with analysis databases because they are considered much less sensitive than those that contain names or other personal identifiers. Analysis data are still considered sensitive, since it may be possible to identify individuals by using particular combinations of reporting system variables. For that reason, analysis data should not be taken home, and all the results of all analyses performed by using reporting system variables must be approved for release as outlined in the surveillance unit's data release policy.

Requirement 27 Access to any secured areas that either contain surveillance data or can be used to access surveillance data by unauthorized individuals can only be granted during times when authorized surveillance or IT personnel are available for escort or under conditions where the data are protected by security measures specified in a written policy and approved by the ORP. (GP-1)

If unauthorized personnel (e.g., cleaning or maintenance crews) are allowed access to the secured area during times when surveillance staff are not present, then more stringent security measures must be employed inside the secured area to meet the program requirements. Under such circumstances, computerized surveillance information and data stored on one or more stand-alone computers or accessible via a LAN-connected workstation must be held securely with access controls in place, such as boot-up passwords that prevent unauthorized access to the computer's hard drive by booting from a system disk, encryption software, or storing the data on removable devices that can be locked away before allowing unauthorized personnel access. If surveillance information is stored on a LAN server, accounts with authorized access should be restricted by time of day and day of week. See Requirement 7.

Managing keys or keypad codes to a secure area is difficult when personnel who receive the keys or codes are not directly supervised by the surveillance unit. Because of staff turnover in cleaning crews, the number of people who may be given keys or codes to the secure area may multiply over time. The more people with keys and codes, the greater the risk to the system. While tracking who has a key or code in this scenario can be difficult, it is recommended that a method of tracking and logging the issuance of keys or codes be implemented. It is further recommended that if an accurate accounting of all keys or codes to a secure area cannot be made, that the lock or code to that area be changed and issued using the tracking and logging method developed.

While many surveillance programs do not routinely grant access to the secured area to cleaning crews or maintenance staff, program requirements can be met even if cleaning crews are granted access without authorized escort, provided added measures (as discussed previously) are employed. The added measures must be named and described in the local security policy. For example, the policy might state that in lieu of escorting cleaning crews and other maintenance staff inside the secured area after hours, the surveillance unit will implement additional documented security measures to provide for enhanced data protection.

Requirement 28 Access to confidential surveillance information and data by personnel outside the surveillance unit must be limited to those authorized based on an expressed and justifiable public health need, must not compromise or impede surveillance activities, must not affect the public perception of confidentiality of the surveillance system, and must be approved by the ORP. (GP-1)

The primary function of HIV/AIDS surveillance is the collection and dissemination of accurate and timely epidemiologic data. Areas that elect to establish linkages to other public health programs for prevention or case management should develop policies

and procedures for sharing and using reported data that ensure the quality and security of the surveillance system. These programs should be developed in consultation with providers and community partners, such as their prevention planning groups. Recipients of surveillance information must be subject to the same training requirements and penalties for unauthorized disclosure as surveillance personnel.

Before establishing any program's linkage to confidential surveillance data, public health officials should define the public health objectives of the linkage, propose methods for the exchange of information, specify the type of surveillance data to be used, estimate the number of persons to be served by the linkage based on the availability of resources, outline security and confidentiality procedures, and compare the acceptability and effectiveness of basing the prevention programs on individual HIV/AIDS surveillance case reports to other strategies. The ORP must have the final approval of proposed linkages, since the ORP is ultimately responsible for any breach of confidentiality.

Prevention programs that use individual HIV/AIDS surveillance case data should evaluate the effectiveness of this public health approach. On an ongoing basis, programs also should assess confidentiality policies, security practices, and any breaches of confidentiality. Individual HIV/AIDS case reports should not be shared with programs that do not have well-defined public health objectives or with programs that cannot guarantee confidentiality.

Requirement 29 Access to surveillance information with identifiers by those who maintain other disease data stores must be limited to those for whom the ORP has weighed the benefits and risks of allowing access and can certify that the level of security established is equivalent to the standards described in this document. (GP-2)

Security is compromised if other programs that lack adequate standards to protect the security and confidentiality of the data are granted access to HIV/AIDS surveillance data or information and use that access to add HIV/AIDS data to their systems.

Linking records from the surveillance data with records from other databases semiannually or annually is encouraged to identify cases not previously reported, such as cases identified through TB surveillance or cancer surveillance. This provides a systematic means to evaluate the performance of health department surveillance and to take action to strengthen weaknesses in systems as they are identified. For example, programs can plan site visits with those providers who do not comply with state reporting laws to stimulate more timely and complete reporting.

Before the linkage of surveillance data, protocols should be discussed and developed. The protocol should address how the linkage will be performed using methods that are secure, who will analyze the results, and how the information will be used to improve the selected surveillance systems.

Requirement 30 Access to surveillance information or data for non-public health purposes, such as litigation, discovery, or court order, must be granted only to the extent required by law. (GP-2)

Some state laws mandate access to HIV/AIDS surveillance information for purposes other than law enforcement or litigation activities. For example, some states require school officials or prospective parents to be notified when they enroll or adopt HIV-infected children. However, the surveillance unit is not necessarily required to release the information just because it is requested by law enforcement or other officials. Access should be granted only to the extent required by law and not beyond any such requirement.

Any request for surveillance information for law enforcement purposes should be reviewed by the ORP with the appropriate program area's legal counsel to determine what specific information, if any, must be released from records maintained solely for epidemiologic purposes. Medical information may be available to the courts from less convenient but more appropriate sources. When information is ordered released as part of a judicial proceeding, any release or discussion of information should occur in closed judicial proceedings, if possible.

Central, Decentral, and Remote Access

The most secure protection for HIV/AIDS surveillance data is having only one centralized database in each state. Centralized data stores are those in which all electronic records of HIV/AIDS cases are stored in only one location within each state. Although not a program requirement, all states currently using the electronic reporting system in more than one location are strongly encouraged to move toward centralized operations where the electronic reporting system is deployed. As new software systems are deployed, CDC will provide technical and financial assistance to facilitate this transition.

Centralization of HIV/AIDS surveillance data within a state has clear benefits. First, centralized data stores offer greater security. Although having several HIV/AIDS surveillance databases throughout a state may have offered advantages in the past, those advantages may be outweighed by the risk of a security breach. Without centralization, most local jurisdictions must either mail copies of case reports to the state or mail external storage devices. Security risks are associated with both methods of data movement.

Centralized data stores add efficiency by improving case matching. With a centralized database, remote surveillance staff may conduct matches against the statewide database, thereby reducing intrastate duplicates and minimizing unnecessary field investigations of cases already reported elsewhere in the state.

Centralized systems may cost less to maintain. States with HIV/AIDS data systems in multiple locations must devote resources for providing technical assistance to surveillance staff at satellite locations. Finally, a centralized platform may support parallel surveillance systems (e.g., TB and STD). In other words, the hardware used for centralized systems could enhance surveillance activities for other diseases without increasing access to the HIV/AIDS database or compromising existing database security in any way.

Technologies such as browser-based applications, the Internet, Wide-Area Networks (WANs), and advances in data encryption technology and firewalls have made centralization of HIV/AIDS surveillance data more feasible.

New browser-based applications have numerous technical access controls, including authentication of the individual attempting access, assignment/restriction of access rights at the variable/field level, and assignment/restriction of access to functional components (role-based privileges). Use of a centralized database allows data entry and data analysis directly from the remote location while preventing access to non-authorized uses. Further, the capacity exists to assign access rights and privileges to staff just as is done in a decentralized system. In addition to these access controls, centralized systems can be configured to limit access by allowing only those connections originating from an authorized person using an authorized workstation.

A centralized database can be accessed using a WAN or the Internet, both of which have advantages and disadvantages. A WAN often uses transmission facilities provided by common carriers, such as telephone companies to establish a dedicated, private, and permanent point-to-point connection between satellite or remote offices and the central database, an option that may be cost-prohibitive for some states. All communications between points must still be password protected, and communications must be encrypted using methods that meet the data encryption standards set forth in this guidance.

Use of the Internet does not require dedicated phone lines and establishes temporary point-to-point connections over a public medium. This would be a less expensive alternative but, because the Internet is a public medium, a Virtual Private Network (VPN) must be established to guard against intrusion during communications. In addition to establishing a VPN, these communications must also be encrypted using methods that meet the data encryption standards set forth in this guidance. Additionally, firewalls must be in place to prevent unauthorized access.

When properly configured, a centralized system allows each local jurisdiction complete access to their HIV/AIDS data while prohibiting access by outside jurisdictions. A local jurisdiction can conduct local-level data analyses directly from a central dataset, or they may download a de-identified dataset for analysis.

If centralization is not yet feasible, each satellite site should maintain only cases within their jurisdiction. For matching case notifications, sites may consider the utility of maintaining limited data on out-of-jurisdiction cases receiving care and/or reported in their jurisdiction. Further, states are encouraged to consider limiting, as much as possible, the number of satellite locations.

Security Breaches

Requirement 31 All staff who are authorized to access surveillance data must be responsible for reporting suspected security breaches. Training of nonsurveillance staff must also include this directive. (GP-3)

Requirement 32 A breach of confidentiality must be immediately investigated to assess causes and implement remedies. (GP-4)

Requirement 33 A breach that results in the release of private information about one or more individuals (breach of confidentiality) should be reported immediately to the Team Leader of the Reporting, Analysis, and Evaluation Team, HIV Incidence and Case Surveillance Branch, DHAP, NCHSTP, CDC. CDC may be able to assist the surveillance unit dealing with the breach. In consultation with appropriate legal counsel, surveillance staff should determine whether a breach warrants reporting to law enforcement agencies. (GP-4)

A breach may be attempted, in progress, done without negative outcome, or done with negative outcome. Attention should be paid to identifying a breach, responding to it, repairing damage, learning from the event, and if necessary revising or enhancing policies and procedures, revising or instituting training, or enhancing physical or operational security.

By keeping a log of breaches and lessons learned from investigating them, the surveillance unit will be able to detect patterns of breaches, track compliance, and incorporate improvements to the security system.

After a breach has been detected, surveillance employees should notify their supervisor who may, depending on the severity of the breach, notify the ORP. Not all security breaches should be reported to CDC. Breaches that do not result in the unauthorized release of private information may be handled at the local/state health department level. However, CDC should be notified of all breaches of confidentiality (i.e., those breaches that result in the unauthorized disclosure of private information with or without harm to one or more individuals). If notified promptly, CDC may be able to provide assistance in responding to the breach in time to avert additional complications both in the state where the breach occurred and in other states. Notification also will allow CDC and the state to give consistent messages when contacted by the media.

Laptops and Portable Devices

Requirement 34 Laptops and other portable devices (e.g., personal digital assistants [PDAs], other hand-held devices, and tablet personal computers [PCs]) that receive or store surveillance information with personal identifiers must incorporate the use of encryption software. Surveillance information with identifiers must be encrypted and stored on an external storage device or on the laptop's removable hard drive. The external storage device or hard drive containing the data must be separated from the laptop and held securely when not in use. The decryption key must not be on the laptop. Other portable devices without removable or external storage components must employ the use of encryption software that meets federal standards. (GP-1)

Laptop computers, PDAs, and other hand-held or portable devices are becoming common tools for HIV/AIDS surveillance and may be key components of centralized surveillance systems. Unfortunately, laptops are vulnerable to theft. Although the likely target of the theft would be the device rather than the data, extreme care must be taken if the device stores HIV/AIDS surveillance data or information. If surveillance data are stored on the device's hard drive, hard drives must be removable and stored

separately when the device is being transported to and from the secured area. Alternatively, a security package that uses both software and hardware protection can be used. For example, an acceptable, though not as robust, level of protection can be achieved by using a smart disk procedure. This procedure prevents the device from booting up unless an encoded smart disk is inserted when the device is first turned on and a password is entered. Such a smart disk must not be stored with the device while in transit. The smart disk must be used in conjunction with an encryption package. Using this kind of protection scheme is critical because the device is capable of containing large amounts of sensitive information (e.g., names, addresses, dates of birth). Therefore, if a device has sensitive data on either an external storage device or hard drive, it must be taken back to the secured area at the close of business (unless out of town business travel is approved). Contingency plans should be in place that outline protective steps to take in case returning to the secure surveillance area is not possible. See Requirement 24 and Requirement 25. A removable drive is worth using even if data are encrypted and the laptop employs several layers of security.

Another option to consider when using laptops is to store encrypted data on an external storage device. If the device is lost or stolen, the data are protected. Unlike the laptop's hard drive, an external storage device lacks market value and is not as likely to be stolen or reused. Nonetheless, external storage devices containing patient identifiers must be encrypted when taken out of a secure area. For more information about removable and external storage devices, refer to section Removable and External Storage Devices.

With the inception of Wireless Fidelity (Wi-Fi) products, many devices can now connect wirelessly to the Internet or a LAN. This functionality introduces risks regarding devices used to collect or store surveillance data. If these devices are not properly configured, data can be transmitted wirelessly over great distances without protection; this can result in the data being exposed to anyone with similar wireless products. Even if data are not being transmitted wirelessly but the device is capable of a wireless connection to the Internet, data stored on the device are susceptible to compromise by exposure to the Internet. For example, surveillance data may be collected in the field and stored on a laptop with Wi-Fi capability. The person collecting the data stops by a store that has a "hot spot" in order to connect to the Internet and check e-mail. The data stored on the laptop have the potential to be compromised. Any use of Wi-Fi or similar evolving wireless technologies must be given serious consideration when developing local policies. CDC strongly recommends that any local policy developed in response to Requirement 34 include explicit language regarding wireless technologies.

Removable and External Storage Devices

Requirement 35 All removable or external storage devices containing surveillance information that contains personal identifiers must

(1) include only the minimum amount of information necessary to accomplish assigned tasks as determined by the surveillance coordinator,

(2) be encrypted or stored under lock and key when not in use, and

(3) with the exception of devices used for backups, devices should be sanitized immediately following a given task.

External storage devices include but are not limited to diskettes, CD-ROMs, USB port flash drives (memory sticks), zip disks, tapes, smart cards, and removable hard drives. Deleting electronic documents does not necessarily make them irretrievable. Documents thought to be deleted often are preserved in other locations on the computer's hard drive and on backup systems. 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). Such physical destruction would include the device, not just the plastic case around the device.

Attachment A

Additional Laptop Security Considerations

Basic Security

Choose a secure operating system and lock it down

An operating system that is secure and offers a secure logon, file level security, and the ability to encrypt data should be used. A password is considered a single-factor authentication process, but for enhanced security, commercial products can be used that change the access to a two-factor authentication. This can be achieved, for example, by using a password and an external device that must be plugged into the USB port. If such a device is used, it should meet federal standards.

Enable a strong BIOS password

The basic input/output system (BIOS) can be password protected. Some laptop manufacturers have stronger BIOS protection schemes than others. In some models, the BIOS password locks the hard drive so it cannot be removed and reinstalled into a similar machine.

Asset tag or engrave the laptop

Permanently marking (or engraving) the outer case of the laptop with a contact name, address, and phone number may greatly increase the likelihood of it being returned if it is recovered by the authorities. A number of metal tamper-resistant commercial asset tags are also available that could help the police return the hardware if it is recovered. Clearly marking the laptops may deter casual thieves.

Register the laptop with the manufacturer

Registering the laptop with the manufacturer will flag it if a thief ever sends the laptop in for maintenance. The laptop's serial number should be stored in a safe place. In the event the laptop is recovered, the police can contact you if they can trace it back to your office.

Physical Security

Get a cable lock and use it

Over 80% of the laptops on the market are equipped with a Universal Security Slot (USS) that allows them to be attached to a cable lock or laptop alarm. While this may not stop determined hotel thieves with bolt cutters, it will effectively deter casual thieves who may take advantage of users while their attention is diverted. Most of these devices cost between $30 and $50 and can be found at office supply stores or online. However, these locks only work if tethered properly to a strong, immovable, and unbreakable object.

Use a docking station

Many laptop thefts occur in the office. A docking station that is permanently affixed to the desktop and has a feature that locks the laptop securely in place can help prevent office theft. If a user is leaving the laptop overnight or for the weekend, a secure filing cabinet in a locked office is recommended.

Lock up the PCMCIA NIC cards

While locking the laptop to a desk with a cable lock may prevent laptop theft, a user can do little to keep someone from stealing the Personal Computer Memory Card International Association (PCMCIA) Network Interface Card (NIC) or modem that is inserted into the side of the machine. These cards can be removed from the laptop bay and locked in a secure location when not in use.

Use a personal firewall on the laptop

Once users connect to the Web from home or a hotel room, their data are vulnerable to attack, as firewall protection provided in the office is no longer available. Personal firewalls are an effective and inexpensive layer of security that can be easily installed. It is recommended that a third-party personal firewall be used to secure workstations.

Consider other devices based on needs

Since laptop use has become common, as has laptop theft, a variety of security-enhancing devices are now available. Motion detectors and alarms are popular items, as are hard drive locks. Biometric identification systems are also being installed on some laptop models, which allow the fingerprint to be the logon ID instead of a password. Cost, utility, and risk need to be taken into account when considering additional devices.

Preventing Laptop Theft

No place is safe

Precautions need to be taken with a laptop regardless of location, as no situation is entirely without risk. As discussed previously, the laptop should always be secured by using a cable lock or secure docking station.

Use a nondescript carrying case

Persons walking around a public place with a leather laptop case can be a target. A form-fitting padded sleeve for the laptop carried in a backpack, courier bag, briefcase, or other common nondescript carrying case may be safer. If a person is traveling in airports and train stations, small locks on the zippers of the case (especially backpacks) can be used (when not passing through security checkpoints) to prevent a thief from reaching into the bag.

Beware of distractions

Business travelers often use cell or pay phones in airports, restaurants, and hotel lobbies. Care needs to be taken that a laptop set down on the floor or a nearby table is not stolen while someone is engrossed in a telephone conversation.

When traveling by air

Sophisticated criminals can prey on travelers. When carrying a laptop, travelers need to use caution to safeguard it. When a person sets a laptop bag down for a minute to attend to other things, there may be a risk of theft. Always be aware of your surroundings because a thief could be waiting for that moment of distraction to grab a laptop (or other valuables).

When traveling by car

When transporting a laptop, it is safer to rent a car with a locking trunk (not a hatchback/minivan/SUV). Regardless of vehicle type, laptops should never be visible from outside of the car. Even when the laptop is in the trunk, the cable lock can be used to secure the laptop to the trunk lid so it cannot be taken easily.

While staying in a hotel

The hazards of leaving valuables in hotel rooms are well documented, and professional thieves know that many business travelers have laptops that can be resold. If a user keeps the laptop in the hotel room, it can be securely anchored to a metal post or fixed object.

Make security a habit

People are the weakest link in the security chain. If a person cares about the laptop and the data, a constant awareness of potential risks will help keep it safe. The laptop should always be locked up when it is not being used or is in storage. (A cable lock takes less time to install than it does for the PC to boot.) Use common sense when traveling and maintain physical contact with the laptop at all times. If a person is traveling with trusted friends or business associates, take advantage of the buddy system to watch each other's equipment.

Protecting Sensitive Data

Use the New Technology File System (NTFS) (proprietary to Windows operating systems)

Assuming a user has Windows NT/2000/XP on the laptop, use the NTFS to protect the data from laptop thieves who may try to access the data. File Allocation Table (FAT) and FAT32 file systems do not support file-level security and provide hackers with an opening into the system.

Disable the guest account

Always double check to make sure the guest account is not enabled. For additional security, assign a complex password to the account and completely restrict logon times. Some operating systems disable the guest account by default.

Rename the administrator account

Renaming the administrator account will stop some hackers and will at least slow down the more determined ones. If the account is renamed, the word 'Admin' should not be in the name. Use something innocuous that does not sound like it has rights to anything. Some computer experts argue that renaming the account will not stop everyone, because some persons will use the Security Identifier (SID) to find the name of the account and hack into it. The SID is a machine-generated, nonreadable binary string that uniquely identifies the user or group.

Consider creating a dummy administrator account

Another strategy is to create a local account named 'Administrator'; then give that account no privileges and a complicated 10+ digit complex password. If a dummy administrator account is created, enable auditing so a user knows when someone has tampered with it.

Prevent the last logged-in user name from being displayed

When a user presses **CTRL+ALT+DEL**, a login dialog box may appear that displays the name of the last user who logged into the computer. This can make it easier to discover a user name that can later be used in a password-guessing attack. This action can be disabled by using the security templates provided on the installation CD-ROM or via Group Policy snap-in. For more information, see Microsoft KB Article Q310125.

Enable EFS (Encrypting File System) in Windows operating systems

Some operating systems ship with a powerful encryption system that adds an extra layer of security for drives, folders, or files. This will help prevent a hacker from accessing the files by physically mounting the hard drive on another PC and taking ownership of files. Be sure to enable encryption on folders, not just files. All files that are placed in that folder will automatically be encrypted.

Disable the infrared port on a user laptop (if so equipped)

Some laptops transmit data via the infrared port on the laptop. It is possible for a person to browse someone else's files by reading the output from the infrared port without the laptop user knowing it. Disable the infrared port via the BIOS, or, as a temporary solution, simply cover it up with a small piece of black electrical tape.

Back up the data before a user leaves

Many organizations have learned that the data on the computer is more valuable than the hardware. Always back up the data on the laptop before a user does any extended traveling that may put the data at risk. This step does not have to take a lot of time, and a user can use the built-in backup utilities that come with the operating system. If the network does not have the disk space to back up all of the traveling laptop user's data, consider personal backup solutions including external hard drives (flash sticks), CD-Rs, and tape backup—all of which can also be encrypted.

Consider using offline storage for transporting sensitive data

Backing up the hard drive before users leave can help them retrieve the data when they return from a trip, but it does not provide an available backup of the data when they are out in the field. Several vendors offer inexpensive external storage solutions that can hold anywhere from 40 MB to 30 GB of data on a disk small enough to fit easily into the pocket. By having a backup of the files users need, they can work from another PC in the event that their laptop is damaged or missing. Most of these devices support password protection and data encryption, so the files will be safe even if a user misplaces the storage disk. When traveling, users should keep these devices with them, not in the laptop case or checked baggage. For additional security, lock or encrypt the files and have them sent by a courier service to the destination hotel or office.

Notes

Attachment B

Additional Security and Policy Considerations

Access and Storage Devices

Establish and implement policies and procedures for using and transporting secure access devices (smart card, key FOB, etc.) and external storage devices (diskettes, USB flash drives, CD-ROM, etc.).

Accountability

Maintain a record of the movements of hardware and electronic media and any persons responsible for transporting these devices.

Application and Data Criticality Analysis

Assess the relative criticality of specific applications and data in support of other contingency plan components.

Audit Controls and Logs

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use protected electronic health information. Establish and implement policies and procedures that regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Establish and implement policies and procedures for the backup, archiving, retention, and destruction of audit logs.

Automatic Logoff

Establish and implement policies and procedures that terminate any electronic session after a predetermined period of inactivity.

Browsers

Establish and implement policies and procedures regarding browser configuration for browser-based applications and Internet usage.

Certificates

Establish server and client digital certificate transportation, generation, and use policies.

Communications

Letterhead stationery, business cards, or dedicated phone lines are used among colleagues for professional purposes, and, in these cases, references to HIV/AIDS would not jeopardize the confidentiality of any case patient. In fact, such identification may be an important part of establishing credibility with providers who report cases. Addressing both purposes (protecting confidentiality and establishing credibility) will require careful organization and perhaps some duplication of communication mechanisms by surveillance

units (e.g., one card and phone line for investigation activities and another set for providers) or the use of more generic terminology (e.g., 'Epidemiology Unit' instead of 'HIV/AIDS Surveillance Unit').

Contingency of Operations and Disaster Recovery

Establish and implement policies and procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

A contingency planning policy and operations policy should address all critical aspects of contingency planning. Storage of data for backup and disaster recovery purposes should have the same if not more stringent accessibility, accountability, and encryption security requirements as a production system.

Along with the above, the following rules should be followed. They may be included in the policy or listed separately:

- Maintain list of all users and applications with access to the data. The list should include (per user or application) the day of week and the hours of the day that access will be needed. Access should be limited to these days and hours. The list should also identify those with access to identifiers.
- Conduct a monthly audit reflecting all successful/unsuccessful access. The report should include day, time of day, and length of access. It should be verified against authorized users and access requirements.
- Define administrative privileges for IT personnel (should be very limited). IT personnel need to have program approval before accessing the data.
- Identify some form of double authentication process for accessing the data.
- Keep systems containing the data in a secured area that is clearly labeled for authorized personnel only.
- Implement column and/or row level encryption of data.
- Create a data backup plan that includes procedures to create and maintain exact copies of protected electronic health information.
- Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity (time-outs).

Emergency Access Procedures

Establish and implement policies and procedures for obtaining necessary protected electronic health information during an emergency.

Emergency Mode Operation

Establish and implement policies and procedures to enable continuation of critical business processes for protecting the security of protected electronic health information while operating in emergency mode.

Encryption and Decryption

Implement a mechanism to encrypt and decrypt protected electronic health information.

Integrity Controls

Implement security measures to ensure that electronically transmitted protected electronic health information is not improperly modified without detection until disposed of. Ensure that any agent, including a contractor or subcontractor to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect the information.

Internet Connectivity

If a modem (internal or external), DSL, or cable is used on a workstation to provide access to the Internet, ensure that passwords and logon data used to access the Internet are not stored on the workstation. Most communications software has the capacity to dial a service and connect a user and even to send a password down the line. To prevent this from happening, never program a password into the workstation.

Some modems have the capability to answer the telephone as well as to make calls. Make sure users know how to tell if their modem has been placed in answering mode and how to turn off that mode. External modems normally have an indicator light labeled AA that glows if Auto Answer mode is selected. Internal modems are harder to monitor, but small utility programs are available that can help. Callback modems actually call the user back at a prearranged number. External modems are recommended because the ease of turning them off offers programs the greatest degree of control.

CDC highly recommends that workstations holding confidential and sensitive data that are connected to the Internet should be disconnected from the Internet except when the Internet is being used for authorized activities.

If the line is for data only, make sure that the telephone number of the line does not appear in the telephone directory and is not displayed on the telephone itself or on the wall socket.

Intrusion Detection

Establish and implement policies and procedures regarding intrusion detection and penetration vulnerabilities.

Keyboard and Screen Locking

Establish and implement policies and procedures for screen saving and keyboard locking.

Logins and Monitoring

Establish and implement policies and procedures for workstation logins, and designate who can request and authorize changes to a login. Establish and implement policies and procedures for monitoring login attempts and reporting discrepancies.

Maintenance Records

Establish and implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).

Media Disposal and Re-use

Establish and implement policies and procedures to address the final disposition of protected electronic health information, and/or the hardware or electronic media on which it is stored. Establish and implement policies and procedures for removal of protected electronic health information from electronic media before the media are made available for re-use.

Networks, LANs, and WANs

Establish and implement policies and procedures governing all servers on the network. Establish and implement policies and procedures for the documentation of network configurations and architectures. Topics to include are

- Name and location of servers
- Netware protocols
- Users, groups, and roles that access data and physical server
- Authentication protocols
- e-mail hosting
- Remote access
- Web hosting
- Data located on each server
- Administrative safeguards

Computers used to maintain HIV/AIDS surveillance information with personal identifiers should not be connected to other computers or computer systems that are located outside of the secure area until and unless the connection is deemed secure by adding multiple layers of protective measures—including encryption software, restricted access rights, and physical protections for the LAN equipment and wiring—and justifying a public health need to maintain highly sensitive data on a system that has multiple users and multiple locations. This system should operate under a certified LAN administrator, who will attest to the system's effectiveness and assume responsibility for any breach of security directly resulting from the system's failure to protect sensitive data.

Internet access devices (e.g., modems and network interface cards) or cables should not be connected to any computer or computer system containing surveillance information and data unless authorized staff need Internet access as a means to enhance surveillance activities. If Internet connectivity is used for surveillance activities, specific rules of use should be provided in writing to authorized users, and they should sign a statement that they understand those rules.

Password Management

Establish and implement policies and procedures for creating, changing, and safeguarding passwords.

Patching and Service Packs

Establish and implement policies and procedures for security patching and service pack control.

Protection from Malicious Software

Establish and implement policies and procedures for guarding against, detecting, and reporting malicious software.

Risk Analysis

Establish and implement policies and procedures that require conducting a regular, accurate, and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of protected electronic health information held by the covered entity.

Routers and Firewalls

Establish and implement policies and procedures regarding router and firewall logs to capture packets that violate filter criteria. Establish and implement policies and procedures for firewall and router configuration.

Software Inventory, Releases, Licensing, and Upgrades

Establish and implement policies and procedures for the inventory of authorized software (including versions) that can be installed on development, training, testing, staging, and production servers and workstations.

Establish and implement policies and procedures for tracking and verifying software licenses.

Establish and implement policies and procedures for prerelease and testing of software. Establish a methodology to deploy new or upgraded software to all appropriate workstations and servers (configuration management). Establish a method for tracking the software loaded on every workstation and server.

Testing and Revision of Plans

Establish and implement policies and procedures for periodic testing and revision of contingency plans.

Transmission Security

Implement technical security measures to guard against unauthorized access to protected electronic health information that is being transmitted over an electronic communications network.

Workstation Use

Establish and implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access protected electronic health information.

Attachment C

Federal Encryption Standards

CDC Policy

Encryption is required when any moderately or highly sensitive files, any moderately or highly critical information, or any limited access/proprietary information is to be transmitted either electronically or physically.

Federal Standards

The National Institute of Standards and Technology (NIST) uses the Federal Information Processing Standards (FIPS) for the Advanced Encryption Standard (AES), FIPS-197. This standard specifies Rijndael as a FIPS-approved symmetric encryption algorithm that may be used by U.S. government organizations (and others) to protect sensitive information. Federal agencies should also refer to guidance from the Office of Management and Budget (OMB).

Advanced Encryption Standard (AES)

Federal Information
Processing Standards Publication 197
November 26, 2001

Name of Standard: Advanced Encryption Standard (AES) (FIPS PUB 197).

Category of Standard: Computer Security Standard, Cryptography.

Explanation: The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that 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 into 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.

Approving Authority: Secretary of Commerce.

Maintenance Agency: Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL).

Notes

Attachment D

CDC Assurance of Confidentiality

ASSURANCE OF CONFIDENTIALITY FOR SURVEILLANCE OF ACQUIRED IMMUNODEFICIENCY SYNDROME (AIDS) AND INFECTION WITH HUMAN IMMUNODEFICIENCY VIRUS (HIV) AND SURVEILLANCE-RELATED DATA (INCLUDING SURVEILLANCE INFORMATION, CASE INVESTIGATIONS AND SUPPLEMENTAL SURVEILLANCE PROJECTS, RESEARCH ACTIVITIES, AND EVALUATIONS)

The national surveillance program for HIV/AIDS is being coordinated by the Surveillance Branch of the Division of HIV/AIDS Prevention - Surveillance and Epidemiology (DHAP - SE), the National Center for HIV/STD/TB Prevention, a component of the Centers for Disease Control and Prevention (CDC), an agency of the United States Department of Health and Human Services. The surveillance information requested by CDC consists of reports of persons with suspected or confirmed AIDS or HIV infection, including children born to mothers infected with HIV, and reports of persons enrolled in studies designed to evaluate the surveillance program. The information collected by CDC is abstracted from laboratory, clinical, and other medical or public health records of suspected or confirmed HIV/AIDS cases; and from surveys that interview persons in recognized HIV risk groups or known to have a diagnosis of HIV/AIDS.

Surveillance data collection is conducted by State and Territorial health departments that forward information to CDC after deleting patient and physician names and other identifying or locating information. Records maintained by CDC are identified by computer-generated codes, patient date of birth, and a state/city assigned patient identification number. The data are used for statistical summaries and research by CDC scientists and cooperating state and local health officials to understand and control the spread of HIV/AIDS. In rare instances, expert CDC staff, at the invitation of state or local health departments, may participate in research or case investigations of unusual transmission circumstances or cases of potential threat to the public health. In these instances, CDC staff may collect and maintain information that could directly identify individuals.

Information collected by CDC under Section 306 of the Public Health Service Act (42 U.S.C. 242k) as part of the HIV/AIDS surveillance system that would permit direct or indirect identification of any individual or institution, on whom a record is maintained, and any identifiable information collected during the course of an investigation on either persons supplying the information or persons described in it, is collected with a guarantee that it will be held in confidence, will be used only for the purposes stated in this Assurance, and will not otherwise be disclosed or released without the consent of the individual or institution in accordance with Section 308 (d) of the Public Health Service Act (42 U.S.C. 242m(d)). This protection lasts forever, even after death.

Information that could be used to identify any individual or institution on whom a record is maintained by CDC will be kept confidential. Full names, addresses, social security numbers, and telephone numbers will not be reported to this national HIV/ AIDS surveillance system. Medical, personal, and lifestyle information about the individual, and a computer-generated patient code will be collected.

Surveillance information reported to CDC will be used without identifiers primarily for statistical and analytic summaries and for evaluations of the surveillance program in which no individual or institution on whom a record is maintained can be identified, and secondarily, for special research investigations of the characteristics of populations suspected or confirmed to be at increased risk for infection with HIV and of the natural history and epidemiology of HIV/AIDS. When necessary for confirming surveillance information or in the interest of public health and disease prevention, 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.

No CDC HIV/AIDS surveillance or research information that could be used to identify any individual or institution on whom a record is maintained, 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; to family members; to parties involved in civil, criminal, or administrative litigation, or for commercial purposes; to agencies of the federal, state, or local government. Data will only be released to the public, to other components of CDC, or to agencies of the federal, state, or local government for public health purposes in accordance with the policies for data release established by the Council of State and Territorial Epidemiologists.

Information in this surveillance system will be kept confidential. Only authorized employees of DHAP - SE in the Surveillance Branch and Statistics and Data Management Branch, their contractors, guest researchers, fellows, visiting scientists, research interns and graduate students who participate in activities jointly approved by CDC and the sponsoring academic institution, and the like, will have access to the information. Authorized individuals are required to handle the information in accordance with procedures outlined in the Confidentiality Security Statement for Surveillance of Acquired Immunodeficiency Syndrome (AIDS) and Infection with Human Immunodeficiency Virus (HIV) and Surveillance-Related Data (Including Surveillance Information, Case Investigations and Supplemental Surveillance Projects, Research Activities, and Evaluations.

Attachment E

Sample Employee Oath - Texas

TEXAS DEPARTMENT OF HEALTH
EMPLOYEE CONFIDENTIALITY AGREEMENT

BACKGROUND INFORMATION:

The Texas Department of Health (TDH) guiding principles establish the paramount importance of patient and client confidentiality in the mission of this department. Information in reports, records, correspondence, and other documents routinely dealt with by employees of the Texas Department of Health may be privileged, confidential, private, or a combination of two or more. In each instance, the information may receive its designation by statute or judicial decision. Such statutes as the *Open Records Act*, *Medical Practice Act*, and the *Communicable Disease Act* contain provisions, which make certain information that comes to TDH privileged and/or confidential.

As a general rule, in transactions carried out on a day-to-day basis, the Medical Practice Act makes medical records and information taken from medical records privileged and confidential. All communicable disease records (STD, HIV, and TB) are made confidential by the Communicable Disease Act. Birth and death records are confidential for 50 years through the provisions dealing with vital statistics in the Open Records Act and other laws. If information is "confidential," it is generally information that should be kept secret and is given only to another person who is in a position of trust. "Privileged" information protects a person who has either given or received confidential information from being revealed in a legal proceeding. Other information that contains "highly intimate or embarrassing facts about a person such that its disclosure 'would be highly offensive to a [reasonable] person...'" and is not of legitimate concern of the public or might hold a person up to the scorn or ridicule of his or her peers if made public, is made confidential by the common law doctrine of the right to privacy [ORD-262, 1980]. Statutes that govern the operation of the department may contain additional provisions that render information that comes into the hands of certain programs in the TDH privileged, confidential, and/or private.

Note to employee: If you have questions regarding confidentiality, you should contact your immediate supervisor or the Office of General Counsel. The signed Employee Confidentiality Agreement will be filed in your personnel folder.

AGREEMENT:

I agree that:

- A patient record or any information taken from a patient record is privileged and confidential. In most instances, such information may not be released unless the person identified in the record provides written consent, or the release of information is otherwise permitted by law. A patient record is defined as: a record of identity and diagnosis of a patient that is initiated and maintained by, or at the direction of a physician, dentist, or someone under the direction or protocols of a physician or dentist.

- I understand that I must not release information from reports, records, correspondence, and other documents, however acquired, containing medical or other confidential information, and that I may not release such information except in a manner authorized by law, such as in a statistical form that will not reveal the identity of an individual or with the written consent of the individual involved.

- I may not release or make public, except as provided by law, Individual case information including demographic data and client contacts.

- I will keep all confidential files, including computer diskettes, in a locked file cabinet when not in use.

- When I am working on a confidential file, I will "lock up" the information when I leave my workstation for lunch, meetings, or for the day. I understand that to "lock up" the information includes *logging off my computer*, not merely saving and closing the confidential file.

- I will keep any confidential files I work with out of the view of unauthorized persons.

- I will not discuss confidential information with people who are not authorized, and/or who do not have a need to know the information.

- When I work with files that contain personal identifiers, I will log off my computer when I am not actively using the file.

- I will conduct telephone conversations and/or conferences, that require the identification of patients by name, in secure areas where the conversation or conference will not be overheard or seen.

- To protect confidentiality, I will not discuss the facts contained in confidential documents in a social setting.

- When transporting information that is privileged, confidential, or private, I will employ appropriate security measures to ensure the material remains protected.

- I will keep information relating to the regulatory activities of the department confidential. Regulatory activities include at least the following: survey schedules, unannounced site visits, survey results, information pertaining to complaints that have been investigated, litigation information, and personnel actions.

- Where applicable, departmental policy requires that personnel have individual passwords to access confidential computer files. I will not use another person's password nor will I disclose my own.

- I understand that my superiors will document any violations of this agreement and he or she will place the documentation in my main personnel file maintained by the Bureau of Human Resources.

- If I am a professional employee (e.g. physician, registered nurse, attorneys, etc.) or I am an employee supervised by or providing support to a professional employee, I understand that I may be subject to additional rules of confidentiality. This agreement does not supersede the code of professional conduct and I further understand that a violation of the code of professional conduct may subject the professional employee to additional sanctions (e.g. loss of license.)

- When I dispose of a document that contains patient information, I will assure that the document is shredded.

I have read this Confidentiality Agreement and I understand its meaning. As an employee of the Texas Department of Health, I agree to abide by the Confidentiality Agreement. I further understand that should I improperly release or disclose privileged, confidential, or private information, I may be subject to an adverse personnel action, up to and including the termination of my employment. I understand that I may be subject to civil monetary penalties, criminal penalties or liability for money damages for such an action.

SIGNATURE:

Employee's Name:_____
Print Employee's Name Date

Employee's Signature:_____

Sample Employee Oath - Seattle/King County

Public Health—Seattle & King County (PH-SKC)
Prevention Division—HIV/AIDS Epidemiology Unit

Confidentiality Agreement

As a PH-SKC employee in the HIV/AIDS Epidemiology Unit, or as a subcontracted employee, student, visiting professional, or work study student, I understand that I may have access to confidential information on persons with reportable diseases, persons counseled during clinical or prevention activities, study participants, or clients of sites involved in our work. This information includes any surveillance- or study-related electronic or paper records or information given orally during an interview or counseling session or through other related contact (e.g., scheduling appointments or updating locators in person or on the phone). Information may also come from records of participating institutions and health care providers, medical/health clinics, drug treatment centers and jails. Examples of confidential information include but are not limited to names, addresses, telephone numbers, sexual and drug-use behaviors, medical, psychological and health-related conditions and treatment, religious beliefs, finances, living arrangements, and social history. **By signing this statement, I am indicating my understanding of my responsibilities and agree to the following**:

- I agree to uphold the confidentiality and security policies specific to my work site(s) and, if required by my work site protocol, to wear my badge that identifies me as a PH-SKC employee when conducting any research, surveillance or prevention activities at field sites outside the office.

- I agree not to divulge, publish, or otherwise make known to unauthorized persons or to the public any information obtained that could identify persons reported with notifiable diseases, persons served during the course of prevention or clinical activities, participants in research or evaluation studies or any information regarding the identity of any patient or client of any institution including any alcohol or drug treatment program to which I have access.

- I understand that all client, patient, and disease report information and records compiled, obtained, or accessed by me in the course of my work are confidential. I agree not to divulge or otherwise make known to unauthorized persons any information regarding the same, unless specifically authorized to do so by office protocol or by a supervisor acting in response to applicable law, court order, or public health or clinical need (WA Administrative Code 246-101-515).

- I understand that I am not to read information and records concerning patients, clients, or study participants, or any other confidential documents, nor ask questions of clients during interviews for my own personal information but only to the extent and for the purpose of performing my assigned duties.

- I understand that a breach of security or confidentiality may be grounds for disciplinary action by PH-SKC, and may include termination of employment.

- I understand that the civil and criminal penalties set forth in the Revised Code of Washington (RCW 70.24.080 and 70.24.084) include, for each breach of STD/HIV records, a fine of $1000 or actual damages for negligent violation and $10,000 or actual damages for intentional or reckless violation, which I would be personally responsible for paying. Breach of other communicable disease records may result in civil penalties imposed by a court and include actual damages and attorneys' fees (RCW 70.02). Alcohol and drug abuse patient records are protected by federal law (42 CFR Part 2) with criminal penalties for violation.

- I understand that action to impose civil or criminal penalties against me may be taken by a prosecuting attorney or another party with standing if I am suspected of being responsible for a breach of confidentiality.

- I agree to notify my supervisor immediately should I become aware of an actual breach of confidentiality or a situation which could potentially result in a breach, whether this be on my part or on the part of another person.

_____

Signature *Date* *Printed name*

_____

Signature of Program Manager *Date* *Printed name*

Sample Employee Oath - Louisiana

STATE OF LOUISIANA
DEPARTMENT OF HEALTH & HOSPITALS

Louisiana Office of Public Health
HIV/AIDS Program

Confidentiality Agreement

As an HIV/AIDS Program employee, subcontracted employee, student, or visiting professional, I understand that I will be exposed to some very privileged patient information. Examples of such information are medical conditions, medical treatments, finances, living arrangements, and sexual orientation. The patient's right to privacy is not only a policy of the HIV/AIDS Program, but is specifically guaranteed by statute and by various governmental regulations.

I understand that intentional or involuntary violation of the confidentiality policies is subject to appropriate disciplinary action(s), that could include being discharged from my position and/or being subject to other penalties. By initialing the following statements I further agree that:
Initial below

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

_____ If in the course of my work I encounter facilities or programs without strict confidentiality protocols, I will encourage the development of appropriate confidentiality policies and procedures.

_____ I will handle confidential data as discretely as possible and I will never leave confidential information in view of others unrelated to the specific activity. I will keep all confidential information in a locked cabinet when not in use. I will encrypt all computer files with personal identifiers when not in use.

_____ I will shred any document to be disposed of that contains personal identifiers. Electronic files will be permanently deleted, in accordance with current HAP required procedures, when no longer needed.

_____ I will maintain my computer protected by power on and screen saver passwords. I will not disclose my computer passwords to unauthorized persons.

_____ I understand that I am responsible for preventing unauthorized access to or use of my keys, passwords, and alarm codes.

_____ I understand that I am bound by these policies, even upon resignation, termination, or completion of my activities.

I agree to abide by the HIV/AIDS Program Confidentiality Policy. I have received, read, understand, and agree to comply with these guidelines.

<u>Warning:</u> Persons who reveal confidential information may be subject to legal action by the person about whom such information pertains.

_____ _____
Signature Date

_____
Printed Name

_____ _____
Supervisor's Signature Date

Notes

Attachment F

Glossary of Surveillance and Technical Terms

Access: The ability or the means necessary to read, write, modify, or communicate data/information. To gain entry to memory in order to read or write data. The entrance to the Internet or other online service or network.

Access control: A cohesive set of procedures (including management, technical, physical, and personnel procedures) that are designed to assure to a given level of reliability that an individual:

1) is the person he or she claims to be (authentication),
2) has a verified public health need to have access to surveillance systems and information,
3) has been authorized to perform the action or access the data, and
4) is doing so from an authorized place using an authorized process.

ACL: Short for AccessControl List, ACL is a listing that tells a computer operating system or other network devices what rights a user has to each item on a computer or network device.

Adware: 1) (ADvertisementWARE) Software that periodically pops up ads in a user's computer. Adware is considered spyware and is installed without the user's knowledge. It typically displays targeted ads based on words searched for on the Web or derived from the user's surfing habits that have been periodically sent in the background to a spyware Web server. 2) (AD supported softWARE) Software that is given away because it contains advertising messages.

Aggregated data: Information, usually summary statistics, that may be compiled from personal information, but is grouped in a manner to preclude the identification of individual cases. An example of properly aggregated data might be, 'Whiteacre County reported 1,234 cases of AIDS during 1997 among Hispanics.' An example of improperly aggregated data might be, 'Blackacre County reported 1,234 cases of AIDS during 1997 among Hispanics and 1 case among American Indians.'

Analysis data, datasets, or database: A dataset created by removing personal data (e.g., names, addresses, ZIP codes, and telephone numbers) so the record or records cannot be linked to an individual, but still allows the remaining data to be analyzed.

Antivirus program: A software program designed to protect a computer and/or network against computer viruses. When a virus is detected, the computer will generally prompt the user that a virus has been detected and recommend an action such as deleting the virus.

Authentication: Verifying the identity of a user who is logging onto a computer system or verifying the origin of a transmitted message. Authentication depends on four classes of data, generally summarized as 'what you know,' 'what you have,' 'what you are,' and 'what you do.'

Authorized access: As determined by the ORP or a designee, the permission granted to individuals to see full or partial HIV/AIDS surveillance information and data that potentially could be identifying or linked to an individual. The ORP or designee should make these determinations according to role-based (or need-to-know) responsibilities.

Authorized personnel: Those individuals employed by the program who, in order to carry out their assigned duties, have been granted access to confidential HIV/AIDS surveillance information. Authorized personnel must have a current, signed, approved, and binding nondisclosure agreement on file.

Availability: The accessibility of a system resource in a timely manner; for example, the measurement of a system's uptime. Availability is one of the six fundamental components of information security.

Biometrics: The biological identification of a person, which includes characteristics of structure and of action such as iris and retinal patterns, hand geometry, fingerprints, voice responses to challenges, and the dynamics of handwritten signatures. Biometrics are a more secure form of authentication than typing passwords or even using smart cards, which can be stolen; however, some forms have relatively high failure rates. Biometric authentication is often a secondary mechanism in two-factor authentication.

Biometric signature: The characteristics of a person's handwritten signature. The pen pressure and duration of the signing process, which is done on a digital-based pen tablet, is recorded as an algorithm that is compared against future signatures.

BIOS (basic input/output system): The built-in software that determines what a computer can do without accessing programs from a disk. On personal computers, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

The BIOS is typically placed in a Read-Only Memory (ROM) chip that comes with the computer (it is often called a ROM BIOS). This ensures that the BIOS will always be available and will not be damaged by disk failures. It also makes it possible for a computer to boot itself. Because Random-Access Memory (RAM) is faster than ROM, many computer manufacturers design systems so that the BIOS is copied from ROM to RAM each time the computer is booted. This is known as shadowing. Many modern PCs have flash BIOS, which means that the BIOS has been recorded on a flash memory chip, which can be updated if necessary.

Breach: A breach is a condition of departure from established policies or procedures. A breach can only be understood in view of a written reference point that describes the desired condition and the link between that condition and the surveillance objectives associated with maintaining the condition. A breach is an infraction or violation of a standard, obligation, or law. A breach in data security would include any unauthorized use of data, even data without names. A breach, in its broadest sense, may be caused by an act of God, a person, or an application/system and may be malicious in nature or purely unintended. An example of a malicious breach would be if staff intentionally, but without authorization, released patient names to the public. An example of an unintended breach would be if completed HIV/AIDS case reports were inadvertently mailed to and read by an unauthorized individual. A breach does not necessarily mean that sensitive information was released to the public or that any one person was harmed. A minor infraction, like forgetting to lock a file drawer containing sensitive information (even if inside a secure area), constitutes a breach of security protocol as compared with a breach of confidentiality.

Other examples of possible breaches:

1) A hacker gains access to an internal machine via the Internet or a dial-up connection.
2) A trusted programmer introduces a program into the production environment that does not behave within expected limits.
3) A technician creates a backdoor into the operation of a system, even for positive and beneficial reasons, that alters the information protection provided.
4) After having been entered into a computerized file, confidential forms are left for removal in the standard paper waste process in an openly accessible location.

Breach of confidentiality: A security infraction that results in the release of private information with or without harm to one or more individuals.

Case-specific information: Any combination of data elements that could identify a person reported to the surveillance system. An example of case-specific information without a name might be, 'A woman with hemophilia from Whiteacre County was diagnosed with AIDS in 1997.'

Certificate: See Digital certificate.

Certification authority or certificate authority: An organization that issues digital certificates (digital IDs) and makes its public key widely available to its intended audience.

Checksum: A value used to ensure data are stored or transmitted without error. It is created by calculating the binary values in a block of data using some algorithm and storing the results with the data. When the data are retrieved from memory or received at the other end of a network, a new checksum is computed and matched against the existing checksum. A nonmatch indicates an error. Just as a check digit tests the accuracy of a single number, a checksum tests a block of data. Checksums detect single bit errors and some multiple bit errors, but are not as effective as the Classes, Responsibilities, and Collaborations (CRC) design method. Checksums are also used by the Sophos antivirus software to determine if a file has changed since the last time it was scanned for a virus.

Ciphertext: Data that have been coded (enciphered, encrypted, encoded) for security purposes. Contrast with plaintext and cleartext.

CISSP: The Certified Information Systems Security Professional (CISSP) exam is designed to ensure that someone handling computer security for an organization or client has mastered a standardized body of knowledge. The certification was developed and is maintained by the International Information Systems Security Certification Consortium (ISC^2). The exam certifies security professionals in 10 different areas:

1) Access control systems and methodology
2) Application and systems development security
3) Business continuity planning & disaster recovery planning
4) Cryptography
5) Law, investigation, and ethics
6) Operations security
7) Physical security
8) Security architecture and models
9) Security management practices
10) Telecommunications and networking security

Cleartext: Same as plaintext.

Confidential information: Any information about an identifiable person or establishment, when the person or establishment providing the data or described in it has not given consent to make that information public and was assured confidentiality when the information was provided.

Confidentiality: The protection of private information collected by the surveillance system.

Confidential record: A record containing private information about an individual or establishment.

Cookies: Data created by a Web server that are stored on a user's computer either temporarily for that session only or permanently on the hard disk (persistent cookie). Cookies provide a way for the Web site to identify users and keep track of their preferences. They are commonly used to maintain the state of the session. The cookies contain a range of Uniform Resource Locators (URLs, or addresses) for which they are valid. When the Web browser or other Hypertext Transfer Protocol (HTTP) application sends a request to a Web server with those URLs again, it also sends along the related cookies. For example, if the user ID and password are stored in a cookie, it saves the user from typing in the same information all over again when accessing that service the next time. By retaining user history, cookies allow the Web site to tailor the pages and create a custom experience for that individual. A lot of personal data reside in the cookie files on the computer. As a result, this storehouse of private information is sometimes the object of attack. A browser can be configured to prevent cookies, but turning them off entirely can limit the Web features. Browser settings typically default to allowing first party cookies, which are generally safe because they are only sent back to the Web site that created them. Third party cookies are risky because they are sent back to sites other than the one that created them. To change settings, look for the cookie options in the Options or Preferences menu within the browser.

Cookie poisoning: The modification of or theft of a cookie in a user's machine by an attacker in order to release personal information. Cookies that log onto password-protected Web sites automatically send username and password. Thieves can thus use their own computers and confiscated cookies to enter victims' accounts.

Cryptography: The conversion of data into a secret code for transmission over a public network. The original text or plaintext is converted into a coded equivalent called ciphertext via an encryption algorithm. The ciphertext is decoded (decrypted) at the receiving end and turned back into plaintext. The encryption algorithm uses a key, which is a binary number that is typically from 40 to 256 bits in length. The greater the number of bits in the key (cipher strength), the more possible key combinations and the longer it would take to break the code. The data are encrypted or locked by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to unlock the code and restore the original data.

Cryptographic key: A numeric code that is used to encrypt text for security purposes.

Data stewards: Refers to individuals responsible for the creation of the data used or stored in organizational computer systems. The data steward determines the appropriate sensitivity and classification level and reviews that level regularly for appropriateness. The data stewards have final responsibility for protecting the information assets and are responsible for ensuring the information assets under their control adhere to local policies. The data steward is one or more of the following:

1) The creator of the information
2) The manager of the creator of the information
3) The receiver of external information
4) The manager of the receiver of the external information

Data user: Anyone who routinely uses the data. Data users are responsible for following operating procedures, taking due care to protect information assets they use, and using computing resources of the department for department purposes only.

Denial of service (DoS): A DoS attack is a form of attacking another computer or organization by sending millions or more requests every second causing the network to slow down, cause errors, or shut down. Because it is difficult for a single individual to generate a DoS attack, these forms of attacks are often created by another organization and/or worms that in turn create zombie computers to create a DoS attack.

DES (Data Encryption Standard): An algorithm that encrypts and decrypts data in 64-bit blocks, using a 64-bit key (although the effective key strength is only 56 bits). It takes a 64-bit block of plaintext as input and outputs a 64-bit block of ciphertext. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm, DES is both a block cipher and a product cipher.

Digital certificate: The digital equivalent of an ID card used in conjunction with a public key encryption system. Also called digital IDs, digital certificates are issued by a trusted third party known as a certification authority or certificate authority (CA) such as VeriSign, Inc. (www.verisign.com). The CA verifies that a public key belongs to a specific organization or individual, and the certification process varies depending on the level of certification and the CA itself. Driver's licenses, notarization, and fingerprints are types of documentation that may be used. The digital certificate typically uses the X.509 file format and contains CA and user information, including the user's public key (details below). The CA signs the certificate by creating a digest, or hash, of all the fields in the certificate and encrypting the hash value with its private key. The signature is placed in the certificate. The process of verifying the signed certificate is done by the recipient's software such as a Web browser or e-mail program. The software uses the widely known public key of the CA to decrypt the signature back into the hash value. If the decryption is successful, the identity of the user is verified. The software then recomputes the hash from the raw data (cleartext) in the certificate and matches it against the decrypted hash. If they match, the integrity of the certificate is verified (it was not tampered with). A signed certificate (the digital certificate) is typically combined with a signed message, in which case the signature in the certificate verifies the identity of the user while the signature in the message verifies the integrity of the message contents. The fact that the message is encrypted ensures privacy of the content. The CA keeps its private key very secure, because if it were ever discovered, false certificates could be created.

Digital signature: A digital guarantee that a file has not been altered, as if it were carried in an electronically sealed envelope. The signature is an encrypted digest (one-way hash function) of the text message, executable or other file. The recipient decrypts the digest that was sent and recomputes the digest from the received file. If the digest matches the file, it is proven to be intact and tamper free as received from the sender.

Disaster recovery: A plan for duplicating computer operations after a catastrophe occurs, such as a fire or earthquake. It includes routine off-site backup as well as a procedure for activating necessary information systems in a new location. The ability to recover information systems quickly after the terrorist attacks of 9/11 proved the value of disaster recovery. Many companies that had programs in place were up and running within a few days in new locations. Companies that did not have disaster recovery systems in place have had the most difficulty recreating their information infrastructure.

Distributed denial of service: On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. A hacker (or cracker) begins a DDoS attack by exploiting vulnerabilities in one computer system and making it the DDoS master. It is from the master system that the intruder identifies and communicates with other systems that can be compromised. The intruder loads cracking tools available on the Internet on multiple (sometimes thousands of) compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service. While the press tends to focus on the target of DDoS attacks as the victim, in reality there are many victims in a DDoS attack including the final target and the systems controlled by the intruder.

Encryption: Encryption is defined as 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, and the 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, under both systems, the larger the key, the more robust the protection.

Encrypting File System (EFS): A feature of the Windows 2000 operating system (and later) that lets any file or folder be stored in encrypted form and decrypted only by an individual user and an authorized recovery agent. EFS is especially useful for mobile computer users, whose computer (and files) are subject to physical theft, and for storing highly sensitive data.

FAT32 (File Allocation Table): The method that the operating systems use to keep track of files and to help the computer locate them on the disk. Even if a file is fragmented (split up into various areas on the disk), the file allocation table still can keep track of it. FAT32 is an improvement to the original FAT system, since it uses more bits to identify each cluster on the disk. This helps the computer locate files easier and allows for smaller clusters, which improves the efficiency of the hard disk. FAT32 supports up to two terabytes of hard disk storage.

Firewall: A method for implementing security policies designed to keep a network secure from intruders. It can be a single router that filters out unwanted packets or may comprise a combination of routers and servers each performing some type of firewall processing. Firewalls are widely used to give users secure access to the Internet as well as to separate an organization's public Web server from its internal network. Firewalls are also used to keep internal network segments secure; for example, the accounting network might be vulnerable to snooping from within the enterprise. In practice, many firewalls have default settings that provide little or no security unless specific policies are implemented by trained personnel. Firewalls installed to protect entire networks are typically implemented in hardware; however, software firewalls are also available to protect individual workstations from attack. While much effort has been made excluding unwanted input to the internal network, less attention has been paid to monitoring what goes out. Spyware is an application that keeps track of a user's Internet browsing habits and sends those statistics to a Web site.

The following are some of the techniques used in combination to provide firewall protection:

1) Network Address Translation (NAT): Allows one Internet Protocol (IP) address, which is shown to the outside world, to refer to many IP addresses internally, one on each client station. Performs the translation back and forth. NAT is found in routers and is built into Windows Internet Connection Sharing (ICS).
2) Packet Filter: Blocks traffic based on a specific Web address (IP address) or type of application (e-mail, File Transfer Protocol [FTP], Web, etc.), which is specified by port number. Packet filtering is typically done in a router, which is known as a screening router.
3) Proxy Server: Serves as a relay between two networks, breaking the connection between the two. Also typically caches Web pages.
4) Stateful Inspection: Tracks the transaction to ensure that inbound packets were requested by the user. Generally can examine multiple layers of the protocol stack, including the data, if required, so blocking can be made at any layer or depth.

IETF (Internet Engineering Task Force): The body that defines standard Internet operating protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP). The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership. Standards are expressed in the form of Requests for Comments (RFC).

Information security: The protection of data against unauthorized access. Programs and data can be secured by issuing identification numbers and passwords to authorized users. However, systems programmers or other technically competent individuals will ultimately have access to these codes. In addition, the password only validates that a correct number has been entered, not that it is the actual person. Using biometric techniques (fingerprints, eyes, voice, etc.) is a more secure method. Passwords can be checked by the operating system to prevent logging in. Database management system (DBMS) software prevents unauthorized access by assigning each user an individual view of the database. Data transmitted over networks can be secured by encryption to prevent eavesdropping. Although precautions can be taken to detect an unauthorized user, it is extremely difficult to determine if a valid user is purposefully doing something malicious. Someone may have valid access to an account for updating, but determining whether phony numbers are entered requires more processing. The bottom line is that effective security measures are always a balance between technology and personnel management.

IPSec (Internet Protocol Security): A security protocol from the IETF that provides authentication and encryption over the Internet. Unlike Secure Sockets Layer (SSL), which provides services at layer 4 and secures two applications, IPSec works at layer 3 and secures everything in the network. Also unlike SSL, which is typically built into the Web browser, IPSec requires a client installation. IPSec can access both Web and non-Web applications, whereas SSL requires a work around for non-Web access such as file sharing and backup. IPSec is supported by IPv6. Since IPSec was designed for the IP protocol, it has wide industry support and is expected to become the standard for virtual private networks (VPNs) on the Internet.

Kerberos: A security system developed at the Massachusetts Institute of Technology that authenticates users. It does not provide authorization to services or databases; it establishes identity at logon, which is used throughout the session.

Key: See Cryptographic key.

Keystroke logger: A program or hardware device that captures every key depression on the computer. Also known as keystroke cops, they are used to monitor an employee's activities by recording every keystroke the user makes, including typos, backspacing, and retyping.

LAN (Local Area Network): Any computer network technology that operates at high speed over short distances (up to a few thousand meters). A LAN may refer to a network in a given department or within a given firm or campus. It differs from computer networks that cross wider geographic spaces such as those networks on a wide area network (WAN). A LAN does not use the public arteries of the Internet like intranets and virtual private networks.

Management controls: Controls that include policies for operating information technology resources and for authorizing the capture, processing, storage, and transmission of various types of information. They also may include training of staff, oversight, and appropriate and vigorous response to infractions.

Need-to-know access: Under exceptional circumstances that are not stipulated in program policies, the case-by-case granting or denying of authorized access to case-specific information. This type of access is not routine; but rather it is for unusual situations and occurs only after careful deliberation by the ORP in concurrence with other public health professionals.

NIST (National Institute of Standards and Technology): Located in Washington, DC, it is the standards-defining agency of the U.S. government; formerly, the National Bureau of Standards. See http://www.nist.gov.

Nonpublic health uses of surveillance data: The release of data that are either directly or indirectly identifying to the public; to parties involved in civil, criminal, or administrative litigation; to nonpublic health agencies of the federal, state, or local government; or for commercial uses.

NTFS (NT File System): One of the file systems for the Windows NT operating system (and later). Windows NT also supports the FAT file system. NTFS has features to improve reliability, such as transaction logs to help recover from disk failures. To control access to files, you can set permissions for directories and/or individual files. NTFS files are not accessible from other operating systems such as DOS. For large applications, NTFS supports spanning volumes, which means files and directories can be spread out across several physical disks.

Overall Responsible Party (ORP): The official who accepts overall responsibility for implementing and enforcing these security standards and who may be liable for breach of confidentiality. The ORP should be a high-ranking public health official, for example, the division director or department chief over HIV/AIDS surveillance. This official should have the authority to make decisions about surveillance operations that may affect programs outside the HIV/AIDS surveillance unit and should serve as one of the contacts for public health professionals and the HIV-affected community on policies and practices associated with HIV/AIDS surveillance. The ORP is responsible for protecting HIV/AIDS surveillance data as they are collected, stored, analyzed, and released and must certify annually that all security program requirements are being met. The state's security policy must indicate the ORP by name.

Patch management: The installation of patches from a software vendor onto an organization's computers. Patching thousands of PCs and servers is a major issue. A patch should be applied to test machines first before deployment, and the testing environments must represent all the users' PCs with their unique mix of installed software.

Personal identifier: A datum, or collection of data, that 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 study data, when taken together, may be used to identify an individual. Therefore, when assembling or releasing databases, it is important to be clear which fields, either alone or in combination, could be used to such ends, and which controls provide an acceptable level of security.

Personnel controls: Staff member controls such as training, separation of duties, background checks of individuals, etc. Compare to physical and technical access controls.

PHIN MS (Public Health Information Network Messaging System): A generic, standards-based, interoperable, and extensible message transport system. It is platform-independent and loosely coupled with systems that produce outgoing messages or consume incoming messages.

Physical access controls: Controls involving barriers, such as locked doors, sealed windows, password-protected keyboards, entry logs, guards, etc. Compare to personnel and technical access controls.

PKI (Public Key Infrastructure): A secure method for exchanging information within an organization, an industry, a nation, or worldwide. A PKI uses the asymmetric encryption method (also known as the public/private key method) for encrypting IDs and documents/messages. Also, see Cryptography. It starts with the certificate authority (CA), which issues digital certificates (digital IDs) that authenticate the identity of people and organizations over a public system such as the Internet. The PKI can also be implemented by an enterprise for internal use to authenticate users that handle sensitive information. In this case, the enterprise is its own CA. The PKI also establishes the encryption algorithms, levels of security, and distribution policy to users. It not only deals with signed certificates for identity authentication, but also with signed messages, which ensures the integrity of the message so the recipient knows it has not been tampered with. The PKI also embraces all the software (browsers, e-mail programs, etc.) that supports the process by examining and validating the certificates and signed messages.

Plaintext: Normal text that has not been encrypted and is readable by text editors and word processors. Contrast with ciphertext.

Private key: The private part of a two part, public key cryptography system. The private key is kept secret and never transmitted over a network.

Project areas: HIV/AIDS surveillance sites that are directly funded by CDC. The HIV/AIDS surveillance project areas are the 50 states, the District of Columbia, San Francisco, Los Angeles, Chicago, Houston, New York City, Philadelphia, Puerto Rico, U.S. Virgin Islands, Guam, American Samoa, the Republic of the Marshall Islands, the Commonwealth of the Northern Mariana Islands, the Republic of Palau, and the Federated States of Micronesia.

Provider: Any source of HIV/AIDS surveillance information, such as a physician, nurse, dentist, pharmacist, or other professional provider of health care or a hospital, health maintenance organization, pharmacy, laboratory, STD clinic, TB clinic, or other health care facility that forwards data into the surveillance system.

Public health uses of surveillance data: The principal public health use of HIV/AIDS surveillance 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 reporting 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.

Surveillance data may be used for public health and epidemiologic research. Data that include names may be collected and released to public health officials on individual cases or clusters of cases of HIV/AIDS that are of particular epidemiologic or public health significance, such as those associated with new or unusual modes of HIV transmission, the detection of unusual strains of HIV, or the occurrence of unusual laboratory or clinical profiles. Analysis of these data may result in the formulation of public health recommendations for standards of diagnosis and treatment of HIV/AIDS and for preventing HIV transmission. However, when such data are released or reported to persons not having role-based or need-to-know access, information shall be presented in such a way as to preclude direct or indirect identification of individuals (e.g., by obscuring geographic or institutional affiliations).

The use of surveillance data to prompt follow-up by health departments with individual patients or their health care providers may constitute legitimate public health practice. In the context that the health department functions as the primary provider of care for persons who seek HIV counseling and testing, diagnosis and treatment of STDs, or medical and social services, health department staff may interact directly with their clients, independently of the role of the health department in monitoring epidemiologic trends in the incidence of HIV/AIDS. Where states or local communities determine that health departments should offer referrals to services for persons whose names are reported to the HIV/AIDS surveillance system and who are not primarily health department clients, and where the surveillance data serve as the source of identification of such individuals, health departments should establish standards and principles for such practice in collaboration with providers and community partners. This helps ensure the security and confidentiality protections are in place.

Public key: The published part of a two part, public key cryptography system. The private part is known only to the owner.

Quality improvement: Activities to enhance the performance level of a process. Quality improvement efforts involve measurement of the current level of performance, development of methods to raise that level, and implementation of those methods.

RAM (Random-Access Memory): A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices, such as printers. There are two basic types of RAM, dynamic RAM (DRAM) and static RAM (SRAM).

The two types differ in the technology they use to hold data, dynamic RAM being the more common type. Dynamic RAM needs to be refreshed thousands of times per second. Static RAM does not need to be refreshed, which makes it faster; but it is also more expensive than dynamic RAM. Both types of RAM are volatile, meaning that they lose their contents when the power is turned off.

Records retention policy: Assigning a length of time and date to paper or electronic records to establish when they should be archived or destroyed.

Risk: In the context of system security, the likelihood that a specific threat will exploit certain vulnerabilities and the resulting effect of that event. A thorough and accurate risk analysis would consider all relevant losses that might be expected if security measures were not in place. Relevant losses can include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures. One of the reasonable risks that are identifiable is that someone could inadvertently or purposely make an unauthorized change to data that could affect patient care. Another reasonable integrity risk is that data may be lost or modified in transmission. Software bugs, viruses and worms, hardware malfunctions, and natural disasters such as fire or flood also can compromise data integrity.

Risk management: The optimal allocation of resources to arrive at a cost-effective investment in defensive measures for minimizing both risk and costs in a particular organization.

Role-based access: Access to specific information or data granted or denied by the ORP depending on the user's job status or authority. Roles typically group users by their work function. This control mechanism protects data and system integrity by preventing access to unauthorized applications. In addition, defining access based on roles within an organization, rather than by individual users, simplifies an organization's security policy and procedures. Compare to need-to-know access.

ROM (Read-Only Memory): Computer memory on which data have been prerecorded. Once data have been written onto a ROM chip, they cannot be removed and can only be read. Unlike main memory (RAM), ROM retains its contents even when the computer is turned off. ROM is referred to as being nonvolatile, whereas RAM is volatile.

Most personal computers contain a small amount of ROM that stores critical programs such as the program that boots the computer. In addition, ROM is used extensively in calculators and peripheral devices such as laser printers, whose fonts are often stored in ROM. A variation of a ROM is a PROM (programmable read-only memory). PROMs are manufactured as blank chips on which data can be written with a special device called a PROM programmer.

RSA (Rivest-Shamir-Adleman): A highly secure cryptography method by RSA Security, Inc., Bedford, MA (www.rsa.com). It uses a two part key. The private key is kept by the owner; the public key is published.

Data are encrypted by using the recipient's public key, which can only be decrypted by the recipient's private key. RSA is very computation intensive; thus it is often used to create a digital envelope, which holds an RSA-encrypted DES key and DES-encrypted data. This method encrypts the secret DES key so that it can be transmitted over the network, but encrypts and decrypts the actual message using the much faster DES algorithm.

RSA is also used for authentication by creating a digital signature. In this case, the sender's private key is used for encryption, and the sender's public key is used for decryption. See Digital signature.

The RSA algorithm is also implemented in hardware. As RSA chips get faster, RSA encoding and decoding add less overhead to the operation.

Sanitize: Also known as disk wiping, sanitizing is the act of destroying the deleted information on a hard disk or floppy disk to ensure that all traces of the deleted files are unrecoverable. Software programs that can successfully sanitize a diskette are available.

Script kiddie: A person who uses scripts and programs developed by others for the purpose of compromising computer accounts and files, and launching attacks on whole computer systems; in general, these persons do not have the ability to write said programs on their own. Normally, this person is someone who is not technologically sophisticated and who randomly seeks out a specific weakness over the Internet to gain root access to a system without really understanding what is being exploited because the weakness was discovered by someone else. A script kiddie is not looking to target specific information or a specific organization, but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability.

Secret key cryptography: Using the same secret key to encrypt and decrypt messages. The problem with this method is transmitting the secret key to a legitimate person who needs it.

Secured area: The physical confinement limiting where confidential HIV/AIDS surveillance data are available. Only authorized staff have access to this area. The secured area usually is defined by hard, floor-to-ceiling walls with a locking door and may include other measures (e.g., alarms, security personnel).

Security: The protection of surveillance data and information systems, with 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.

Server farm: A group of network servers that are housed in one location. A server farm provides bulk computing for specific applications such as Web site hosting; in contrast, although a data center has many servers, it also has people. In a server farm, a user would generally only see a technician when an installation or a repair was performed; whereas in the data center, operators would be sitting at consoles, putting paper in printers, and possibly moving disks and tapes from one place to another. A server farm is typically a room with dozens, hundreds, or even thousands of rack-mounted servers humming away. They might all run the same operating system and applications and use load balancing to distribute the workload between them.

Smart cards: A credit card sized card with a built-in microprocessor and memory used for identification or financial transactions. When inserted into a reader, it transfers data to and from a central computer. It is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times. As a financial transaction card, it can be loaded with digital money and used like a travelers check, except that variable amounts of money can be spent until the balance is zero.

Spyware: Software that sends information about Web surfing habits to its Web site. Often quickly installed on a computer in combination with a free download purposefully selected from the Web, spyware (also known as parasite software or scumware) transmits information in the background as a user moves around the Web.

The license agreement may or may not clearly indicate what the software does. It may state that the program performs anonymous profiling, which means that a user's browsing habits are being recorded. Such software is used to create marketing profiles. For example, a person who accesses Web site A, often accesses Web site B and so on. Spyware can be clever enough to deliver competing products in real time. For example, if a user accesses a Web page to look for a minivan, an advertisement for a competitor's minivan might pop up.

Spyware organizations argue that as long as they are not recording names and personal data, but treat the user as a numbered individual who has certain preferences, they are not violating a person's right to privacy. Nevertheless, many feel their privacy has been violated. The bottom line is that once users detect a spyware program in their computer, it can be eliminated, albeit sometimes with much difficulty. The downside is that people can become suspect of every piece of software they install.

SSL (Secure Sockets Layer): The leading security protocol on the Internet. When an SSL session is started, the server sends its public key to the browser, which the browser uses to send a randomly generated secret key back to the server in order to have a secret key exchange for that session. Developed by Netscape, SSL has been merged with other protocols and authentication methods by the IETF into a new protocol known as Transport Layer Security (TLS).

Super user: Someone with the highest level of user privilege who can allow unlimited access to a system's file and setup. Usually, super user is the highest level of privilege for applications, as opposed to operating or network systems. A super user could destroy the organization's systems maliciously or simply by accident.

Surveillance: The ongoing and systematic collection (paper or electronically), analysis, and interpretation of health data in the process of describing and monitoring a health event. This information is used for planning, implementing, and evaluating public health interventions.

Surveillance data: Statistics generated from disease surveillance in either paper or electronic format.

Surveillance information: Details collected on an individual or individuals for completing routine or special surveillance investigations. Examples of HIV/AIDS surveillance information are the HIV/AIDS report forms, ancillary notes about risk investigations and related questionnaires, notes about suspect cases, laboratory reports, ICD9/10 line lists, discharge summaries, death certificates, and drug data stores.

Symmetric encryption: Same as secret key cryptography.

Technical access controls: Controls involving technology, such as requirements for password use and change, audit of the electronic environment, access to data controlled through known software tools, and control over introduction of changes to the information technology environment (hardware, software, utilities, etc.). Compare to personnel and physical access controls.

Trojan horse: A program that appears legitimate, but performs some illicit activity when it is run. It may be used to locate password information, make the system more vulnerable to future entry, or simply destroy programs or data on the hard disk. A Trojan horse is similar to a virus, except that it does not replicate itself. It stays in the computer doing its damage or allowing somebody from a remote site to take control of the computer. Trojans often sneak in attached to a free game or other utility.

Two-factor authentication: The use of two independent mechanisms for authentication; for example, requiring a smart card and a password. The combination is less likely to allow abuse than either component alone.

Virus: Software program first written by Fred Cohen in 1983, and later coined in a 1984 research paper. A virus is a software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. Installing an antivirus protection program can help prevent viruses.

VPN (Virtual Private Networks): A network that is connected to the Internet, but uses encryption to scramble all the data sent through the Internet so the entire network is "virtually" private.

Vulnerability: A security exposure in an operating system or other system software or application software component. Security firms maintain databases of vulnerabilities based on version number of the software. Any vulnerability can potentially compromise the system or network if exploited. For a database of common vulnerabilities and exposures, visit http://icat.nist.gov/icat.cfm.

WAN (Wide Area Network): A network of computers that can span hundreds or thousands of miles. Unlike intranets and virtual private networks, a WAN does not use public Internet arteries and is isolated from the public domain.

Zombie: A computer system that has been covertly taken over to transmit phony messages that slow down service and disrupt the network. A pulsing zombie sends bogus messages in periodic bursts rather than continuously.

Notes

Attachment G

Using HIV Surveillance Data to Document Need and Initiate Referrals

Contents

Toolkit 5 **Using HIV Surveillance Data**

Introduction to the Issue

The primary objective of population-based HIV case surveillance is to allow state and local health departments to monitor changing trends in the HIV epidemic and thereby direct available resources to where they are needed most. For this purpose, CDC strongly recommends the use of summary statistics with identifying information removed. This Toolkit provides information and resources to help HIV/AIDS surveillance coordinators develop principles for the use of the HIV/AIDS surveillance database to document need and evaluate services.

Although the HIV surveillance system was not designed for case management purposes, some states and territories have chosen to use individual case reports to offer HIV-infected individuals referrals to voluntary prevention and care services. States that are using the HIV surveillance database for this purpose should follow established guidelines and standards for maintaining security and confidentiality of HIV surveillance information. States implementing HIV case surveillance and considering using case reports as a basis for offering voluntary referrals to prevention and treatment programs should do so only when principles and practices are developed locally in collaboration with community partners. The collaborative process should include developing explicit protocols with appropriate clearances that establish practices for contacting providers and patients and ensure that security and confidentiality protections are in place if information from HIV/AIDS surveillance is used to initiate any contact with patients.

Finally, both CDC and CSTE have stated that partner counseling and referral services (PCRS), formerly known as partner notification, activities do not necessarily have to be linked to HIV reporting in order to be effective public health tools. All states currently conduct partner notification activities regardless of whether they have HIV surveillance. Furthermore, some states have initiated HIV surveillance exclusive of PCRS programs. Therefore, CDC and CSTE suggest support for voluntary PCRS should be developed in the broader context of HIV prevention community planning or other advisory processes and should not be necessarily coupled with HIV surveillance. If established, linkages of surveillance and prevention services should neither compromise the quality and security of the surveillance system nor compromise the quality, confidentiality, and voluntary nature of prevention services.

This Toolkit can help guide discussions between surveillance staff and prevention programs and community advisory groups on the ways in which information from the HIV/AIDS surveillance database may be used as a mechanism for referring HIV-infected individuals to prevention, medical, and social services when areas decide to do so locally. The various HIV-related services that patients and their providers may choose are described. In addition, the Toolkit outlines some issues that should be considered before making the decision to use HIV surveillance in this way, suggests alternative strategies, and outlines a process for deliberations.

Using HIV Surveillance Data **Toolkit 5**

This Toolkit:

- reviews in question and answer format some issues surveillance staff and stakeholders must consider when discussing how HIV/AIDS surveillance data may be used to provide referrals for HIV-related prevention and medical services, and
- provides materials that may be useful in discussions with stakeholders.

The *Resource Manual's Appendix*, bound separately, contains the following background resources that provide more comprehensive information on the issues and on current CDC guidelines and practices:

- CDC. Public health uses of HIV-infection reports—South Carolina, 1986-1991. *Morbidity and Mortality Weekly Report* 1992;41(15):245-249. (Located in the Toolkit 1 section of the Appendix.)
- CDC. U.S. Public Health Service Recommendations for human immunodeficiency virus counseling and voluntary testing for pregnant women. July 7, 1995. *Morbidity and Mortality Weekly Report* 44 (No. RR-7).
- CSTE. National HIV Surveillance: Addition to the National Public Health Surveillance System. 1997 CSTE Annual Meeting Position Statement #ID-4. (Located in the Toolkit 1 section of the Appendix.)
- Fenton KA, Peterman TA. HIV partner notification: taking a new look. *AIDS* 1997;11(13):1535-1546.
- West GR, Stark KA. Partner notification of HIV prevention: a critical reexamination. *AIDS Education and Prevention* 1997;9(Supplement B):68-78.

In addition, surveillance coordinators may want to consult these two resources, which CDC has distributed separately:

- CDC. *Draft HIV Partner Counseling and Referral Services Operational Guidelines*. October, 1998.
- CDC. *HIV Prevention Case Management—Guidance*. September 1997.

Background Information for the Surveillance Coordinator

As surveillance officers and their staffs work with prevention programs and community representatives, they may receive questions about how individual surveillance data may be used by health departments for purposes of referral to services or other program activities. This section provides background information, organized by questions that may be raised, to help surveillance staff explain CDC recommendations, discuss the implications and answer questions about the issues.

☞ This symbol points out further supporting materials contained in Toolkit 5 or directs the reader to related materials in other Toolkits.

How should HIV/AIDS surveillance data be used?

HIV and AIDS data should be used to monitor changing epidemiologic trends in incidence and outcomes, assist in formulating public health policy, document the need for services, and direct available resources for targeted prevention interventions for persons with HIV. This is done through the use of aggregate data. Aggregate data include summary statistics compiled from personal information, but grouped to preclude identification of individual cases. For example, the number and characteristics of persons living with HIV by geographic area may be used to determine the distribution of local care services or assess the need for drug assistance programs. HIV data may also be used to set priorities among areas and groups at risk that might benefit from targeted HIV testing and counseling programs.

Together with local community advisory groups, health departments may determine that another appropriate use of surveillance data is to use individual-level data from HIV surveillance registries to prompt follow up by the health department with patients or providers to offer voluntary referrals for various patient services. Individual-level data include case specific data where individuals are identified. There is no CDC requirement that surveillance programs share individual case reports with prevention or care programs. To be consistent with the federal assurance of confidentiality under which CDC collects HIV/AIDS surveillance data and the purpose for which CDC provides support to states to conduct HIV/AIDS surveillance, individual-level surveillance data should not be used to directly or indirectly identify an individual for non-public health purposes, such as the release of individual-level data to the public, to parties involved in civil, criminal, or administrative litigation, or to non-health agencies of the federal, state, or local government.

☞ *Using HIV Surveillance Data: Focus on New Jersey* is a handout that summarizes that state's experiences using aggregate HIV surveillance data for planning and policy purposes.

What types of patient services might patients be referred to through the use of individual case reports?

This might include a wide range of care services, such as medical treatment, social or support services, or laboratory testing, including CD4+T-lymphocyte testing. In addition, prevention services, such as assistance with notifying sex and needle-sharing partners, prevention case management, and counseling and testing services, may also be offered.

What are partner counseling and referral services (PCRS) and how are they carried out?

The goals of PCRS are to provide services to sex and needle-sharing partners of HIV-infected individuals and to help partners gain access to individualized counseling, testing, medical evaluation, treatment, and other prevention services. It is a means of alerting individuals who may not know they have been exposed to HIV through sexual contact or needle-sharing practices to the possible need for testing and medical services. It also is a means of reaching individuals early in the disease process so they are able to more quickly take advantage of new therapies for treatment of HIV infection and opportunistic infections. Prevention education and risk reduction services are also important for those exposed to HIV to help prevent further spread in the community.

Partners may be notified either by the individual who has been diagnosed with HIV, by his or her health care provider, or by a health professional from the health department. HIV infected persons do not have to reveal their partners to their physicians or to the health department to receive needed medical services. In many cases, the individual is coached on ways to notify his or her own partners and provided with information that partners will need to seek testing and other services.

If partners are contacted by health department staff, they are referred to testing and other support services, and their confidentiality is under the same laws, rules, and mechanisms that apply to HIV-infected individuals. Partners' decisions to seek services are entirely voluntary. For more detailed information on PCRS, surveillance coordinators can contact the CDC Community Assistance, Planning, and National Partnerships Branch (CAPNP) HIV prevention project officer, who can provide copies of the *Draft HIV Partner Counseling and Referral Service Operational Guidelines*—October 7 1998.

What is HIV prevention case management?

HIV Prevention Case Management (PCM) is a client-centered HIV prevention activity with the goal of promoting the adoption and maintenance of HIV risk-reduction behaviors by clients with multiple complex problems and risk-reduction needs. It is a hybrid of HIV risk reduction counseling and traditional case management that includes intensive, ongoing, individualized prevention counseling, support, and service brokerage. CDC provides funding and technical assistance for individual-level health education and risk-reduction activities, including PCM. Guidance for planning, implementing, and evaluating PCM is provided in *HIV Prevention Case Management-Guidance. September 1997*., which may be obtained through the CDC National AIDS Clearinghouse at 1-800-458-5231.

How do some health departments use individual HIV case reports to initiate referrals for prevention and medical services?

Some states have instituted local policies that allow individual case reports to be used to trigger follow-up activities by the health department in which individuals are referred to prevention and treatment services. Areas with these linkages primarily do so to facilitate offering services to persons tested in non-public health clinic settings, because follow up with health department clients (i.e., persons tested in public STD clinics or counseling and testing sites) to provide referrals to appropriate prevention and care services is routine. Contacting non-health department reporting sources (e.g., hospitals, private physicians, clinics, or blood banks) may be done to provide training and education regarding conduct of PCRS, provide information about available services, or seek permission to contact patients.

Because the majority of persons reported with HIV infection are tested in medical settings (not public health clinics), areas considering offering referrals for services (e.g., PCRS) based on surveillance case reports should carefully consider if there is a need to follow up with patients tested and reported by private providers (e.g., private physicians, HMOs). Offering assistance with post-test counseling or referrals to test providers that do not routinely provide medical or prevention services (e.g., blood banks or laboratories) may also be considered. Policies regarding contact by health department staff of persons tested in non-health department settings should be developed locally by health departments in collaboration with communities and providers. For health department staff to directly contact patients tested by a non-health department provider without first contacting that provider may be seen as intrusive and be an inefficient use of public health resources. Follow up by health department staff of persons reported with HIV should be conducted with the participation of the physician or provider who ordered the HIV antibody test. In some states, the health department must always obtain permission from the HIV-infected individual's physician before contacting that person. Although surveillance staff may inquire about the patient's need for services and referrals while following up on case reports or when obtaining complete data (e.g., risk information) from a provider, surveillance staff should not be responsible for contacting patients to provide these referrals. Rather, health department staff who are responsible for PCRS or patient case management should initiate the contact following locally established procedures. The figure on page 5-9 diagrams an example of how this contact should take place.

Some examples of locally developed procedures for using individual case reports to initiate patient services include:

In Minnesota, all persons testing HIV positive are contacted by health department staff and provided, on a voluntary basis, with referrals for case management, assistance with obtaining Medicaid and drug assistance, and partner notification services. After receiving HIV positive reports from laboratories and other sources, surveillance provides information to designated prevention staff who then coordinate contact with patients. Information from surveillance is provided on a case-by-case basis to prevention staff at weekly sessions using a confidential process. HIV prevention staff try to work with providers to ensure that the doctor or doctor's staff has a chance to discuss health

department support services with the patient first. This gives the patient some advance notice to expect a contact from the health department and an opportunity to ask questions of a familiar provider. This discussion may relieve some of the anxiety or fear that individuals may experience when health department contact is unexpected or not understood. HIV surveillance and prevention staff believe this increases patient and provider cooperation with health department programs.

- In Missouri, the health department seeks permission from providers before contacting patients tested in the private sector. Surveillance staff obtain physician approval to contact a patient tested in and reported from the private sector while they are obtaining information that was not included with the original case report. If the provider thinks follow up with the patient is appropriate, surveillance staff share the individual case report with designated heath department staff, who distribute cases for follow up to local field investigators. Disease investigators offer PCRS and inform the patient about the availability of "service coordination" in their state.

  - ☞ *Frequently Asked Questions about HIV Surveillance and its Relationship to Prevention and Treatment Services* is a handout that describes surveillance's links to services and partner notification.

What are CDC's recommendations regarding the use of HIV surveillance data for referrals to patient services, such as prevention case management or PCRS?

CDC maintains that individual HIV case data need not be used directly to initiate prevention or patient services. Rather, aggregate surveillance data can be used to direct non-surveillance health department staff (e.g., case managers, disease investigators) to providers or reporting sources to advise them of available prevention and services for their patients. If providers ask for assistance, areas should follow locally-established protocols and procedures to respond to provider and patient needs.

Ultimately, CDC considers the decision to use HIV surveillance to initiate case management services or referrals to other services to be a local decision. If established, these linkages should not compromise the quality or security of the surveillance system nor compromise the quality, confidentiality, and voluntary nature of prevention case management or other services. Methods undertaken should not jeopardize support for representative, complete, and timely case reporting or be inconsistent with CDC required standards for security and confidentiality of HIV/AIDS surveillance data. If areas, with the concurrence of community planning groups, elect to share individual case data from surveillance with other programs, the recipients of the surveillance information should be subject to the same penalties for unauthorized disclosure as are surveillance personnel. In addition, prevention programs that use HIV surveillance case data should evaluate the effectiveness of this approach and the program's policies and practices that protect against breaches of confidentiality.

☞ See *Security Standards for Protection of HIV/AIDS Surveillance Information and Data*. *Appendix C: Guidelines for HIV/AIDS Surveillance—1998* for information regarding security and confidentiality standards for HIV data.

What issues should health departments and communities consider before making the decision to use confidential information obtained through HIV/AIDS surveillance for PCRS or case management services?

There are two key issues that health departments should consider before deciding to use data for PCRS or case management:

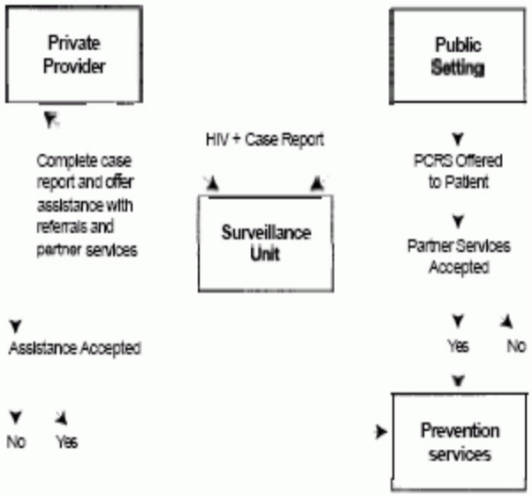
Whether linking surveillance for referrals to patient services may affect the acceptability of the system. Linking HIV surveillance to services may adversely affect the acceptability of HIV surveillance by the community and providers because it may be perceived as an unauthorized release of information from the surveillance system. One way of increasing acceptability may be to involve physicians in the process. For example, if case reports result in referrals from surveillance to other health department staff for the purpose of offering prevention services, health care providers should be contacted before notifying the patient and offered an opportunity to say whether follow up with the individual is appropriate or necessary. Physicians should be encouraged to counsel their patients about the probability of a health department visit (as local policy dictates) so the patient can be prepared for or expect the initial contact and understand its purpose. In one state, the patient is given the option of calling appropriate health department staff himself or herself and is therefore put in control of the process. This option enables the patient to preserve his or her confidentiality.

Whether there are alternative strategies for offering PCRS or case management that might be more feasible, timely, and efficient and that do not require the use of individual HIV/AIDS case reports. HIV surveillance and PCRS activities do not need to be linked in order to be effective public health tools. For example, focusing PCRS activities or referrals to other services in places where clients are present at public clinics and counseling and testing sites may be more efficient programmatically, less intrusive to individuals, ensure more timely provision of such services, and does not require a direct link to surveillance case reports. Public health providers can then ensure discussion of the PCRS process during pretest counseling in a controlled and confidential environment. Focused PCRS activities may facilitate client-centered counseling methods and allow for better referrals to treatment and other care services. Another strategy that does not require linkage to surveillance might include providing targeted testing services in high prevalence areas. Areas may also choose to target education to large providers of HIV care and assist in developing mechanisms of referral for health department services when needed. In some states, health department staff train physicians to provide partner services and referrals and only contact the provider's patients at the provider's request.

What steps should local areas take when developing appropriate procedures for using surveillance data to initiate referrals to patient services?

If a health department and community together decide to use surveillance data to initiate PCRS or case management, they should discuss the flow of information in detail, develop a protocol, and conduct a pilot of the proposed system. (The figure shows an example of information flow in public and private settings.) The protocol should include objectives and cover practical considerations such as what information will be released, who will have access to it, what security measures will be in place (particularly if information is shared outside of surveillance), and how the system will be evaluated. Data should not be shared with programs that do not have well defined public health objectives or with programs that cannot guarantee confidentiality. Prevention programs that receive surveillance information must be subject to the same penalties for unauthorized disclosure as are surveillance programs, and they must maintain the shared data in a secure and confidential manner. At a minimum, areas should develop a written protocol, and pilot test the system in one or two areas before widespread implementation to ensure procedures are appropriate, and that the system achieves stated goals and objectives and is acceptable to providers and the community.

Example of Information **Flow** for Case Reports and Service Referrals from Public and Private Settings



Are health department staff required to contact those who are reported through HIV surveillance?

There is no federal requirement that health department staff contact HIV-infected individuals or their sex or needle-sharing partners. However, as a condition of HIV prevention funding, CDC requires all state HIV prevention programs to "establish standards, implement, and maintain procedures for confidential, voluntary, client-centered counseling and referral of sex and needle-sharing partners of HIV infected persons, consistent with the current CDC Partner Counseling and Referral Services Guidance" and "maintain their good faith effort to notify spouses of infected persons as required by law and as certified to CDC" regardless of the state's HIV reporting laws. CDC and CSTE have stated that HIV surveillance and PCRS activities do not need to be linked in order to be effective public health tools.

Using HIV Surveillance Data:

Focus on New Jersey

New Jersey was the first state with high HIV prevalence to include HIV reporting in its surveillance system. New Jersey added HIV surveillance to its existing AIDS surveillance system in October 1991 and began reporting case data in January 1992. Since that time, the state has used aggregate HIV surveillance data to improve its ability to monitor the epidemic. In turn, this enhanced monitoring capability has allowed public health workers to better target prevention and treatment services for HIV-infected people, and also has served as a basis for policy decisions and program evaluation.

Improved Prevention Planning and Priority Setting

Surveillance data are used to inform the community prevention planning process. Community planning groups, made up of local representatives from public health and community organizations serving persons with HIV and members of the infected community, currently dictate the targeted populations and geographic distribution of funded activities for street and community outreach, health education risk reduction sessions, and prevention case management. Surveillance data help planners set priorities and reassess need for services in their communities.

Bridgeton, New Jersey is a classic example of the use of HIV data in prevention planning. According to AIDS reports from Bridgeton through 1997, women accounted for 24% of the patients, men accounted for 76% of the patients and the 20- to 29-year-old age range accounted for only 9% of the patients.

However, as shown here, HIV data showed a completely different picture. According to HIV reports from Bridgeton, women accounted for 43% of the cases, men accounted for 57% of the cases, and the 20- to 29-year-old age range accounted for 39% of the patients, making it the age range with the largest number of cases. The HIV data provided a more accurate picture of where the epidemic existed and where it was headed. In contrast, AIDS information showed only where the epidemic had been.

Brighton, NJ: Data through 12/31/97

	AIDS Data	HIV Data
Women	24%	43%
Men	76%	57%
20-29 Year Olds	9%	39%

Based on the information provided by HIV surveillance data, Bridgeton initiated a targeted prevention program for younger women and youth. It includes multiple ongoing small group sessions and prevention case management for women and youth.

Resource Management and Funding Allocation

Drug Assistance. Many states have been concerned that adding new antiretroviral therapies to their AIDS drug distribution program would drain resources and necessitate limiting enrollment into the program. When the question of adding these new medications to New Jerseys drug assistance program arose, the state was able to base its decision, in part, on an economic model formulated from the estimated number of people in New Jersey living with HIV or AIDS. HIV surveillance provided critical data on the potential number of infected persons and the percentage that would be eligible for the program. While many states have had to modify their eligibility criteria, New Jersey was able to add all of the new antiretroviral agents and remain solvent without modifying the eligibility criteria.

Better Directing of Treatment Resources. The number of people living with HIV and AIDS is used for planning purposes because it provides a more accurate representation of the number of people who will require care in a specific geographic area. New Jersey and other states are working toward a more equitable overall funding of Ryan White money per case.

5-10

Evaluation of Perinatal Prevention Efforts

Evaluating Public Health Recommendations. HIV data have played an important role in evaluating the implementation of the public health service recommendations for the prevention of mother-to-infant (perinatal) HIV transmission in New Jersey. Because New Jersey has name-based HIV reporting, public health officials have been able to follow children who were exposed to HIV perinatally to determine their final HIV status. Aggregate HIV surveillance data have been used to monitor Zidovudine (ZDV) use in pregnant women and subsequent trends in perinatal transmission. The percentage of children infected as a result of perinatal HIV exposure in New Jersey decreased from 22% in 1993 to 15% in 1995. HIV data also indicated that the HIV status of 96% of HIV positive pregnant women was known at or before birth.

Argue Against Mandatory Testing. HIV data have been used to inform the Medical Society of New Jersey and the New Jersey legislature, the Governors AIDS Advisory Council, and the National Academy of Sciences/Institute of Medicine Committee on Perinatal HIV Transmission, that the New Jersey law requiring mandatory HIV counseling and voluntary testing for all pregnant women appears to be working well in New Jersey, and there is no need for mandatory testing of newborns.

Tracking Emerging Issues of Public Health Importance

Monitoring Recent Infection. HIV surveillance data are used to characterize persons likely to have recently acquired their HIV infection based on documented recent seroconversion, persons with high CD4 counts, and young persons recently diagnosed with HIV. Aggregate HIV surveillance data in New Jersey are used to help identify where new infections may be occurring and describe risk exposure associated with recent infection. HIV data on persons with recent HIV infection in New Jersey is being used to guide more focused research on circumstances surrounding testing, previous sexual and drug-using behaviors that may have been associated with HIV transmission, as well as current behaviors among persons with recent HIV infection.

Keeping a Watch for Unusual HIV Strains. HIV, a pathogen that mutates extensively, presents significant challenges to effective disease control. In the United States, the most common HIV strain is identified as HIV-1, Group M, Subtype B. Data from New Jerseys HIV surveillance system formed the basis of special studies to detect variant strains of HIV in the state. The first U.S. case of HIV-2, a type primarily found in West Africa, was identified in New Jersey through the surveillance system. An additional study led to the identification of variant strains of HIV in the state. Information from HIV surveillance provided public health officials with the basic information to guide development of a separate system to detect variant strains of HIV, and this is now in place in New Jersey. Understanding variations of HIV will help ensure that diagnostic tests will be able to detect the virus both for proper testing and to protect the safety of the blood supply.

Frequently Asked Questions on HIV Surveillance and its Relationship to Prevention and Treatment Services

How should HIV/AIDS surveillance data be used to direct services?

In addition to monitoring changing epidemiologic trends, HIV and AIDS data should be used to assist in formulating public health policy, documenting the need for services, and directing available resources for targeted prevention interventions for persons with HIV. This is done through the use of summary HIV data. For example, the number and characteristics of persons living with HIV by geographic area may be used to determine the distribution of local care services or assess the need for drug assistance programs. HIV data may also be used by communities and health officials to set priorities among areas and groups at risk that might benefit from targeted HIV testing and counseling programs, redistribution of drug assistance programs, or community outreach and education programs.

When people with HIV are reported to the health department, do they automatically get prevention and treatment services?

No. There is no automatic or recommended link between HIV surveillance and prevention services. All states have programs in place to offer voluntary partner counseling and referral services (PCRS) regardless of whether the state requires HIV reporting or not. In addition, some states also offer referrals for treatment services to patients seen within the public health clinic system.

Some states use HIV case data to trigger referrals of individuals to services. However, the extent to which individual HIV case data are used to facilitate access to prevention and care services varies from state to state, depending on factors such as resources, the available array of services, and community concerns about release of confidential information for purposes other than surveillance.

What is the linkage between HIV surveillance programs and HIV prevention case management and care programs?

CDC considers that the decision to link surveillance with case management services should be made at the local level and should be developed in the broader context of HIV prevention community planning or other advisory processes. If established, these linkages should not compromise the quality or security of the surveillance system nor compromise the quality, confidentiality, and voluntary nature of prevention case management services. Although CDC is not directly responsible for the delivery of medical care for persons with HIV, CDC does provide funds for state and local programs to facilitate the referral from HIV counseling and testing programs and health education risk reduction programs to HIV care facilities.

How do some health departments use HIV case reports to assist in offering referrals to services?

Prevention services and referrals are routinely offered to persons testing HIV positive in health department clinics and counseling and testing sites. However, the extent to which health departments use HIV data to assist in offering services to persons tested in other settings varies. When persons are reported with HIV from non-health department providers, such as physicians and HMOs, health departments offer services through or with the participation of the physician or provider who ordered the HIV antibody test. For example, health department staff may contact the provider to offer information on services available to their patient or they may discuss meeting with their patient if appropriate. In these areas, health department staff always obtain permission from the HIV-infected individuals physician before contacting the person directly.

Attachment H

Security and Confidentiality Program Requirement Checklist

State:_____ Site:_____

Person completing form_____ Date:_____

Guiding Principles

Guiding Principle 1 HIV/AIDS surveillance information and data will be maintained in a physically secure environment. Refer to sections Physical Security and Removable and External Storage Devices.

Guiding Principle 2 Electronic HIV/AIDS surveillance data will be held in a technically secure environment, with the number of data repositories and individuals permitted access kept to a minimum. Operational security procedures will be implemented and documented to minimize the number of staff that have access to personal identifiers and to minimize the number of locations where personal identifiers are stored. Refer to sections Policies, Training, Data Security, Access Control, Laptops and Portable Devices, and Removable and External Storage Devices.

Guiding Principle 3 Individual surveillance staff members and persons authorized to access case-specific information will be responsible for protecting confidential HIV/AIDS surveillance information and data. Refer to sections Responsibilities, Training, and Removable and External Storage Devices.

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

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

Requirements

(Initial items as completed)

___ **Requirement 1:** **Policies must be in writing. (GP-2)**

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

___ **Requirement 3:** **A policy must describe methods for the review of security practices for HIV/AIDS surveillance data. Included in the policy should be a requirement for an ongoing review of evolving technology to ensure that data remain secure. (GP-5)**

___ **Requirement 4:** **Access to and uses of surveillance information or data must be defined in a data release policy. (GP-2)**

___ **Requirement 5:** **A policy must incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying. (GP-2)**

___ **Requirement 6:** **Policies must be readily accessible by any staff having access to confidential surveillance information or data at the central level and, if applicable, at noncentral sites. (GP-2)**

___ **Requirement 7:** **A policy must define the roles for all persons who are authorized to access what specific information and, for those staff outside the surveillance unit, what standard procedures or methods will be used when access is determined to be necessary. (GP-2)**

___ **Requirement 8:** **All authorized staff must annually sign a confidentiality statement. Newly hired staff must sign a confidentiality statement before access to surveillance data is authorized. The new employee or newly authorized staff must show the signed confidentiality statement to the grantor of passwords and keys before passwords and keys are assigned. This statement must indicate that the employee understands and agrees that surveillance information or data will not be released to any individual not granted access by the ORP. The original statement must be held in the employee's personnel file and a copy given to the employee. (GP-2)**

___ **Requirement 9:** **A policy must outline procedures for handling incoming mail to and outgoing mail from the surveillance unit. The amount and sensitivity of information contained in any one piece of mail must be kept to a minimum. (GP-2)**

___ **Requirement 10:** **In compliance with CDC's cooperative agreement requirement, the ORP must certify annually that all program requirements are met. (GP-2)**

___ **Requirement 11:** **Each member of the surveillance staff and all persons described in this document who are authorized to access case-specific information must be knowledgeable about the organization's information security policies and procedures. (GP-3)**

___ **Requirement 12:** **All staff who are authorized to access surveillance data must be responsible for challenging those who are not authorized to access surveillance data. (GP-3)**

___ **Requirement 13:** **All staff who are authorized to access surveillance data must be individually responsible for protecting their own workstation, laptop, or other devices associated with confidential surveillance information or data. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data. Staff must take care not to infect surveillance software with computer viruses and not to damage hardware through exposure to extreme heat or cold. (GP-3)**

___ **Requirement 14:** **Every individual with access to surveillance data must attend security training annually. The date of training must be documented in the employee's personnel file. IT staff and contractors who require access to data must undergo the same training as surveillance staff and sign the same agreements. This requirement applies to any staff with access to servers, workstations, backup devices, etc. (GP-3)**

___ **Requirement 15:** **All physical locations containing electronic or paper copies of surveillance data must be enclosed inside a locked, secured area with limited access. Workspace for individuals with access to surveillance information must also be within a secure locked area. (GP-1)**

___ **Requirement 16:** **Paper copies of surveillance information containing identifying information must be housed inside locked filed cabinets that are inside a locked room. (GP-1)**

___ **Requirement 17:** **Each member of the surveillance staff must shred documents containing confidential information before disposing of them. Shredders should be of commercial quality with a crosscutting feature. (GP-3)**

___ **Requirement 18:** **Rooms containing surveillance data must not be easily accessible by window. (GP-1)**

___ **Requirement 19:** **Surveillance information must have personal identifiers removed (an analysis dataset) if taken out of the secured area or accessed from an unsecured area. (GP-1)**

___ **Requirement 20:** **An analysis dataset must be held securely by using protective software (i.e., software that controls the storage, removal, and use of the data). (GP-1)**

___ **Requirement 21:** **Data transfers and methods for data collection must be approved by the ORP and incorporate the use of access controls. Confidential surveillance data or information must be encrypted before electronic transfer. Ancillary databases or other electronic files used by surveillance also need to be encrypted when not in use. (GP-1)**

___ **Requirement 22:** **When case-specific information is electronically transmitted, any transmission that does not incorporate the use of an encryption package meeting the Advanced Encryption Standard (AES) encryption standards and approved by the ORP must not contain identifying information or use terms easily associated with HIV/AIDS. The terms HIV or AIDS, or specific behavioral information must not appear anywhere in the context of the communication, including the sender and/or recipient address and label. (GP-2)**

___ **Requirement 23:** **When identifying information is taken from secured areas and included on line lists or supporting notes, in either electronic or hard copy format, these documents must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any information that could easily be associated with HIV or AIDS. (GP-1)**

___ **Requirement 24:** **Surveillance information with personal identifiers must not be taken to private residences unless specific documented permission is received from the surveillance coordinator. (GP-1)**

___ **Requirement 25:** **Prior approval must be obtained from the surveillance coordinator when planned business travel precludes the return of surveillance information with personal identifiers to the secured area by the close of business on the same day. (GP-1)**

___ **Requirement 26:** **Access to any surveillance information containing names for research purposes (that is, for other than routine surveillance purposes) must be contingent on a demonstrated need for the names, an Institutional Review Board (IRB) approval, and the signing of a confidentiality statement regarding rules of access and final disposition of the information. Access to surveillance data or information without names for research purposes beyond routine surveillance may still require IRB approval depending on the numbers and types of variables requested in accordance with local data release policies. (GP-1)**

___ **Requirement 27:** **Access to any secured areas that either contain surveillance data or can be used to access surveillance data by unauthorized individuals can only be granted during times when authorized surveillance or IT personnel are available for escort or under conditions where the data are protected by security measures specified in a written policy and approved by the ORP. (GP-1)**

___ **Requirement 28:** **Access to confidential surveillance information and data by personnel outside the surveillance unit must be limited to those authorized based on an expressed and justifiable public health need, must not compromise or impede surveillance activities, must not affect the public perception of confidentiality of the surveillance system, and must be approved by the ORP. (GP-1)**

___ **Requirement 29:** **Access to surveillance information with identifiers by those who maintain other disease data stores must be limited to those for whom the ORP has weighed the benefits and risks of allowing access and can certify that the level of security established is equivalent to the standards described in this document. (GP-2)**

___ **Requirement 30:** **Access to surveillance information or data for nonpublic health purposes, such as litigation, discovery, or court order, must be granted only to the extent required by law. (GP-2)**

___ **Requirement 31:** **All staff who are authorized to access surveillance data must be responsible for reporting suspected security breaches. Training of nonsurveillance staff must also include this directive. (GP-3)**

___ **Requirement 32:** **A breach of confidentiality must be immediately investigated to assess causes and implement remedies. (GP-4)**

___ **Requirement 33:** **A breach that results in the release of private information about one or more individuals (breach of confidentiality) should be reported immediately to the Team Leader of the Reporting, Analysis, and Evaluation Team, HIV Incidence and Case Surveillance Branch, DHAP, NCHSTP, CDC. CDC may be able to assist the surveillance unit dealing with the breach. In consultation with appropriate legal counsel, surveillance staff should determine whether a breach warrants reporting to law enforcement agencies. (GP-4)**

___ **Requirement 34:** **Laptops and other portable devices (e.g., personal digital assistants [PDAs], other handheld devices, and tablet personal computers [PCs]) that receive or store surveillance information with personal identifiers must incorporate the use of encryption software. Surveillance information with identifiers must be encrypted and stored on an external storage device or on the laptop's removable hard drive. The external storage device or hard drive containing the data must be separated from the laptop and held securely when not in use. The decryption key must not be on the laptop. Other portable devices without removable or external storage components must employ the use of encryption software that meets federal standards. (GP-1)**

___ **Requirement 35:** **All removable or external storage devices containing surveillance information that contains personal identifiers must:**

(1) include only the minimum amount of information necessary to accomplish assigned tasks as determined by the surveillance coordinator,

(2) be encrypted or stored under lock and key when not in use, and

(3) with the exception of devices used for backups, devices should be sanitized immediately following a given task. Before any device containing sensitive data is taken out of the secured area, the data must be encrypted. Methods for sanitizing a storage device must ensure that the data cannot be retrievable using Undelete or other data retrieval software. Hard disks that contained identifying information must be sanitized or destroyed before computers are labeled as excess or surplus, reassigned to nonsurveillance staff, or before they are sent off-site for repair. (GP-1)