



Guide to HIV Surveillance in California

California Department of Public Health
Center for Infectious Diseases
Office of AIDS
HIV/AIDS Surveillance Section
MS 7700
P.O. Box 997426
Sacramento, CA 95899-7426

Version 3.5

October 2014

Version #	Revision Date	Summary of Changes	Revised By
1.0	5/2009	Initial draft	Ann Nakamura
1.5	3/2010	Updates made	Brian Bannister
2.0	5/2011	Revisions made as required	Steven Starr
2.5	3/2012	Significant revisions completed to match the new S&C Guidelines	Steven Starr
3.0	6/2014	Revisions made as required	Chris Unzueta & Cullen Fowler-Riggs
3.5	10/2014	Significant revisions made	Scott Masten & Cullen Fowler-Riggs

Table of Contents

I.	Introduction	4
II.	Case Finding	7
III.	Pediatric Surveillance	11
IV.	Death Ascertainment	12
V.	Security and Confidentiality	13
VI.	National HIV/AIDS Program Standards	13
VII.	Federal and State Statutes or Regulations	14
VIII.	Surveillance Activities	16
IX.	Movement of Confidential Materials	22
X.	Data Release	23
XI.	Security Breaches	23
XII.	Special Investigations	24
XIII.	Statutes and Regulations	26
XIV.	COPHICases Overview	26
XV.	HIV/AIDS Case Procession	28
XVI.	Matching HIV/AIDS Reports	29
XVII.	Case Checks	29
XVIII.	Processing Laboratory Reports	30
XIX.	HIV/AIDS Case Reporting	30
XX.	HIV/AIDS Case Updates, Edits, and Deletions	33
XXI.	Data Quality Control	34
XXII.	Data Accuracy	34
XXIII.	Reporting Performance Measures	35
XXIV.	eHARS Disaster Recovery Plan	40
XXV.	Acronyms	42

I. Introduction

Core HIV/AIDS Surveillance

HIV/AIDS surveillance is generally defined as the systematic collection, analysis, interpretation, dissemination, and evaluation of population-based information about persons with diagnosed HIV and AIDS. HIV/AIDS surveillance data include all demographic groups and are the primary source of population-based HIV/AIDS information available in all U.S. states and territories.

HIV and AIDS cases are defined according to the prevailing Centers for Disease Control and Prevention (CDC) surveillance case definitions. HIV/AIDS surveillance in clinical settings that involves the reporting of confidential HIV tests and AIDS diagnoses is sometimes called “core” or “case” surveillance. Core surveillance is one of many forms of HIV/AIDS surveillance that have been funded by CDC to monitor the HIV/AIDS epidemic in the United States. Examples of other HIV/AIDS surveillance programs funded by CDC include surveillance of new HIV infections (incidence surveillance); HIV risk behaviors (behavioral surveillance); quality of care and clinical outcomes (medical morbidity monitoring); and perinatal HIV transmission (enhanced perinatal surveillance). Core HIV/AIDS surveillance is the focus of this guide and the term, “HIV/AIDS surveillance” is used throughout this document to refer to core surveillance activities.

The objective of HIV/AIDS surveillance is to provide precise and timely information necessary to identify ongoing patterns of infection and to measure the burden of HIV. CDC receives HIV/AIDS case reports from all 50 states, the District of Columbia, U.S. dependencies and possessions, and independent nations. CDC maintains the national HIV/AIDS surveillance dataset and provides funding and technical assistance to health departments for HIV/AIDS surveillance activities.

Analysis of HIV/AIDS case records provides de-identified information needed to describe and monitor health trends, allocate resources, and to facilitate research. HIV/AIDS surveillance data are routinely used for surveillance reports, HIV epidemiologic profiles, and HIV prevention grant applications. At the federal level, the Health Resources and Services Administration (HRSA) uses HIV and AIDS core surveillance data from CDC to determine funding levels for Parts A and B of the Ryan White HIV/AIDS Treatment Modernization Act (TMA). CDC reviews HIV/AIDS reports received from state health departments for accuracy and completeness, and then provides HRSA with HIV and AIDS case counts for states and eligible metropolitan areas (EMAs).

The Ryan White TMA is the largest source of federal funding for people living with HIV/AIDS (PLWH/A) in the United States. Through the Ryan White TMA, California receives funding for a wide variety of health care and support services, which identify and coordinate efforts to assist California’s most vulnerable HIV-positive populations.

The California Department of Public Health, Center for Infectious Diseases, Office of AIDS

The California Department of Public Health (CDPH), Center for Infectious Diseases, Office of AIDS (OA) is designated by the California Health and Safety Code (HSC) Section 131019, as the lead agency responsible for coordinating state programs, services, and activities relating to HIV/AIDS. The mission of OA is to:

- assess, prevent, and interrupt the transmission of HIV and provide for the needs of infected Californians by identifying the scope and extent of HIV infection and the needs which it

creates, and disseminating timely and complete information; assure high-quality preventive, early intervention, and care services that are appropriate, accessible, and cost effective;

- promote the effective use of available resources through research, planning, coordination, and evaluation; and
- provide leadership through a collaborative process of policy and program development, implementation, and evaluation.

OA's HIV/AIDS Surveillance Section

OA's HIV/AIDS Surveillance Section (Surveillance Section) is organized under the Surveillance, Research, and Evaluation Branch. The Surveillance Section is a confidential, central surveillance of demographic and clinical information on all reported HIV infections and AIDS cases in California. To ensure that HIV/AIDS case reporting is consistent with California law and that the statewide system meets federal program performance standards, the Surveillance Section provides local health jurisdictions (LHJs) with support and training for developing, maintaining, and enhancing HIV/AIDS surveillance programs.

HIV/AIDS Case Reporting in California

Over the years, surveillance of HIV/AIDS has evolved to adapt to changes in the HIV/AIDS epidemic and advances in diagnosis and treatment. In the beginning of the epidemic, surveillance systems across the country only reported AIDS cases. Surveillance later expanded due to increased understanding of the etiology and transmission of AIDS to include HIV reporting. Confidential AIDS case reporting, by name, began in California in 1983. HIV reporting was first implemented on July 1, 2002, using non-name codes, and using names on April 17, 2006.

In California and the rest of the United States, HIV infections and AIDS diagnoses are reported through a combination of passive and active surveillance. Passive surveillance is conducted through state required reporting of HIV and AIDS cases by health care providers and reporting of HIV-positive test results from laboratories to LHJs. Active surveillance is accomplished through routine visits to hospitals, physician offices, laboratories, counseling and testing (C&T) clinics, and outpatient clinics to ensure completeness, timeliness, and accuracy of reported data. In California and other states, HIV/AIDS surveillance has historically relied heavily upon active case surveillance, through on-site chart reviews and case report completion by local surveillance staff at the health care provider's office.

To improve timeliness and completeness of reporting and ensure prompt identification and response to emerging problems in the field, OA supports a decentralized reporting system where HIV and AIDS case reports are identified through passive and active surveillance efforts coordinated by California's 61 LHJs. HIV/AIDS surveillance case data and laboratory reports, reported to LHJs by health care providers and laboratories, is then sent to the HIV/AIDS Surveillance Section via the Lab Data Entry Tool (LDET) or on the Adult Case Report Form (ACRF). The Surveillance Section surveillance coordinators review the ACRFs for accuracy and then input the information into the Enhanced HIV/AIDS Reporting System (eHARS), and in turn, submit electronic HIV/AIDS case reports, without personal identifiers, to CDC.

California's HIV/AIDS reporting practices are based on OA's legislatively-mandated responsibilities; specific California laws governing HIV reporting; and on federal CDC Program Requirements (PRs). CDC provides federal funding to U.S. states and territories for HIV/AIDS surveillance programs in order to meet the goals and objectives of the national HIV/AIDS surveillance program. At the federal level, the HIV Incidence and Case Surveillance Branch

(HICSB) of the Divisions of HIV/AIDS Prevention (DHAP), National Center for HIV, STD, and TB Prevention (NCHSTP), is responsible for conducting national HIV/AIDS surveillance and ensuring that CDC-funded HIV/AIDS surveillance programs provide complete, timely, and accurate HIV/AIDS case reporting.

CDC is authorized under Sections 317(k) (2) (c) and (d) of the Public Health Service Act, [Title 42, United States Code, Section 247b (k) (2) (c) and (d)] and is charged with monitoring disease reporting at the national level. As such, CDC has the authority to allocate funding for, and evaluate the performance of HIV/AIDS surveillance programs of, local and state health departments. The Chief of OA serves as the Overall Responsible Party (ORP) for CDC-funded surveillance activities in California and provides oversight of statewide reporting activities.

Purpose of the Guide

Readily available documentation of surveillance procedures, developed in accordance with California laws and regulations, helps ensure that surveillance activities are consistent with state legal requirements. Moreover, written documentation of HIV/AIDS surveillance procedures satisfies many CDC structural requirements, process standards, and outcome standards.

In order to foster uniformity in HIV/AIDS surveillance data quality from states and territories in the United States, and to ensure that all funded programs are in compliance with federal requirements, CDC, in collaboration with the Council of State and Territorial Epidemiologists (CSTE), developed the *Technical Guidance for HIV/AIDS Surveillance Programs* as a guide for state and local HIV/AIDS surveillance programs. The Technical Guidance includes a collection of outcome standards, process standards, structural requirements, and performance requirements.

- **Outcome standards** (sometimes called “performance standards”) are quantifiable and are used to assess the quality of HIV/AIDS data. For example, CDC uses outcome standards for completeness, timeliness, duplication, risk, and death ascertainment to measure the quality of HIV/AIDS case data reported by states and territories to the national HIV/AIDS surveillance system.
- **Process standards** refer to specific activities that are either recommended or required to achieve outcome standards. Ensuring that all HIV/AIDS Case Report Forms are visually inspected is one example of a process standard.
- The term, “**structural requirements**” is used to describe what a program needs to have in order to operate an HIV/AIDS surveillance system. For example, HIV/AIDS Case Report Forms are a structural requirement necessary to conduct HIV/AIDS surveillance that is consistent with CDC policies and practices.
- Security and confidentiality **performance requirements (PRs)** are designed protect the national system from program practices that are potential security breaches. PRs are mandatory and must be certified by the ORP as a condition of funding.

Technical assistance and training are available from both the Surveillance Section and CDC to guide local HIV/AIDS surveillance practice. However, policies and procedures that meet area-specific legal and operational needs must be developed by local programs.

California, as a CDC-funded HIV/AIDS surveillance program, is responsible to CDC and HICSB and must ensure that statewide HIV/AIDS case data meets CDC performance requirements. This guide is designed to complement CDC’s and CSTE *Technical Guidance for HIV/AIDS Surveillance Programs, Volumes I – III* and provides the blueprint for California statewide

operations in accordance with State legislative mandates, regulations, and CDC policies.

This guide has three purposes: 1) to describe the California HIV/AIDS surveillance system; 2) to enhance the Surveillance Section's quality assurance efforts; and 3) to assist local HIV/AIDS surveillance programs in developing area-specific procedures for local program operations that meet CDC performance requirements.

II. Case Finding

Chapter Summary

The term, case finding, describes the system for identifying all reportable HIV infections and AIDS diagnoses. The case finding process depends on accurate tracking of reporting trends, particularly from key reporting sources.

HIV infections and AIDS diagnoses are reported to LHJs through a combination of passive and active surveillance. Therefore, collaboration is the cornerstone of successful surveillance programs. Passive surveillance is conducted throughout the state and requires reporting of HIV and AIDS cases by health care providers and reporting of HIV-positive test results from laboratories to LHJs. A well-functioning passive surveillance system relies on periodic visits to reporting sources by surveillance staff. Improving the quality of passive reporting can also reduce the amount of active surveillance required of surveillance staff.

Active surveillance depends on effective collaboration between health care providers, laboratories, and LHJs. LHJ staff often provide technical assistance, training, and support to health care providers for legally-mandated HIV/AIDS reporting activities. Active surveillance is accomplished through routine visits to hospitals, physician offices, laboratories, C&T clinics, and outpatient clinics to ensure completeness, timeliness, and accuracy of reported data. In California, complete and timely HIV/AIDS surveillance has depended on active case surveillance, through on-site chart reviews and case report completion by local surveillance staff at health care providers' offices.

This chapter primarily provides information necessary to identify potential sources of HIV and AIDS case reports. Topics addressed in this chapter include:

- identification of reporting sources and access to source data;
- surveillance considerations for incarcerated individuals;
- reportable events;
- pediatric HIV/AIDS surveillance;
- death ascertainment; and
- reporting tools.

Key State Statutes or Regulations

Provisions of the California Health and Safety Code (HSC) establish the legal authority of public health agencies to investigate the nature of HIV exposures. Under HSC Section 120125, CDPH is required to examine the causes of communicable diseases occurring or likely to occur in California. Upon being informed by a local health officer of any contagious, infectious, or communicable disease, CDPH is authorized to take necessary measures to ascertain the nature of the disease and prevent its spread (HSC Section 120140).

HSC Section 131019 establishes OA as the lead agency within the state, responsible for coordinating state programs, services, and activities relating to HIV and AIDS. HSC Section 121022 requires health care providers and laboratories to report cases of HIV to LHJs by name, and LHJs to report cases of HIV by name to OA. Reporting requirements for health care providers, laboratories, and LHJs are operationalized in California Code of Regulations (CCR), Title 17.

Case Finding Activities

HIV/AIDS surveillance systems rely on the quality and completeness of case reports received from health care providers and laboratories. LHJs generally receive HIV test reports passively from laboratories and obtain HIV/AIDS case reports from local health care providers through active surveillance efforts.

Active Surveillance

Active surveillance often includes assisting providers with reporting of cases, particularly when providers are having difficulty meeting or are not yet familiar with reporting requirements. Contacting providers and laboratories to strengthen disease reporting is a core public health activity and often includes providing assistance with reporting cases.

In California, an important function of LHJ surveillance staff has been to assist reporting sources with completing the necessary forms, gathering demographic data, and recording patient history and treatment. Local surveillance programs are encouraged to contact reporting providers, schedule site visits to discuss appropriate reporting procedures, and offer ongoing assistance, when possible. To maintain relationships between LHJs and local health care providers, and to identify any problems with reporting, OA encourages LHJ staff to visit all large reporting sites frequently.

In addition to providing on-site assistance, it is important for LHJs to maintain frequent and regular communication with specific reporting sources. A well-functioning surveillance system relies on periodic visits by surveillance staff to all reporting sources. Providing feedback on quality and level of reporting will help health care providers better understand disease trends within the populations they serve and identify any surveillance-related issues that need improvement.

Correctional Facilities

Federal, state, and local correctional institutions located within each LHJ should be included in regular surveillance activities. Reporting sources include not only prisons, but also city and county jails. The California Department of Corrections and Rehabilitation (CDCR) has separate detention facilities for adults and juveniles, so surveillance activities should include facilities within both the adult and juvenile justice systems. CDCR oversees state prisons, camps, community correctional facilities, and prisoner mother facilities. Juveniles can be incarcerated in a county ranch, camp, or in a California Youth Authority institution.

Not all county or city jails offer HIV testing, and sometimes records are no longer available after a prisoner is released. Therefore, it is important to determine the availability of HIV testing and/or medical treatment for detainees within each LHJ. Medical care for prisoners may be provided on-site, by contract with a local acute care facility, or at a correctional medical facility run by the State (such as in Vacaville, Solano County). Surveillance activities should be coordinated through the institution's chief medical officer.

Surveillance Considerations for Incarcerated Individuals

Avoiding duplication can be particularly challenging when conducting surveillance activities in jails and prisons. It is not uncommon for individuals to be housed in several correctional facilities before completing their sentences. For this reason, timely reporting is critically important. Due to court-ordered testing or outreach and testing services, HIV reports may be received by LHJs for individuals awaiting trial in county or city jails. If convicted, prisoners could then be transferred to a state prison, which may not be located in the same LHJ as the local jail.

Newly convicted prisoners may also be sent to a reception center before they are transferred to the prison where they will complete their sentences. Reception centers receive a large number of prisoners from facilities throughout the state and perform a variety of assessments to determine the individual needs of prisoners. It is not uncommon for an individual to be tested in the county jail and tested again shortly after entering the reception center. Both institutions, to comply with reporting laws, report the HIV-positive test results to their LHJ, which results in duplication.

Vital Statistics

Death certificate review is a routine HIV/AIDS case finding method. At the State level, CDPH's Office of Vital Records maintains a uniform system for registration and centralized surveillance of all deaths that occur in California. Vital statistics registries in LHJs maintain records on every death occurring in the jurisdiction.

The official death certificate lists basic demographic information, where the death occurred, the immediate cause of death, underlying cause of death, and associated conditions. The completeness of the death record depends on the physician or medical examiner who completes the document. Routine death certificate reviews offer an opportunity to follow up on the dates of death and localities in which the deaths occurred for all persons diagnosed with HIV/AIDS.

Most LHJ HIV/AIDS surveillance programs have links with vital statistics surveillance staff to obtain copies of death certificates where HIV or opportunistic infections associated with AIDS are indicated. Maintaining a close relationship with vital statistics surveillance staff may help identify previously unreported cases and will also provide LHJ surveillance staff with timely mortality information on reported cases.

Hospital Outpatient Settings

When AIDS was first recognized in 1981, acute care hospitals were the primary treatment sites and, therefore, the primary source for case reports. The advent of highly active antiretroviral therapy in 1996 allowed many HIV-infected individuals to be treated through outpatient services. Decreased hospitalization has shifted reporting from hospital-based acute care settings to outpatient clinics and laboratories.

The administration of hospital-affiliated outpatient clinics varies widely. When initiating surveillance in these settings, it is important to first meet with the administrator for all of the associated clinics. There may be differences between inpatient and outpatient settings in medical record storage and access, laboratory testing and notification arrangements, and communicable disease reporting procedures. It is important to determine if there is a person designated as the primary contact for reporting communicable diseases. This individual is generally responsible for assuring compliance with reporting regulations and ensuring that reporting is occurring from all available sources within the organization.

It is also important to understand how outpatient clinics are organized and to determine where HIV/AIDS patients are likely to be seen. For example, patient care may or may not be monitored in a medical clinic that specializes in HIV care. LHJ surveillance staff should be aware of any outpatient clinics for infectious disease, dermatology, oncology, respiratory disease, or neurology. All such clinics may treat patients with HIV.

Private Laboratories

As with hospital laboratories, private laboratories—whether they are located in California or not—are required to report specific information regarding all confirmed HIV tests based on samples that originated from California to the local health officer in the California jurisdiction where the ordering health care provider is located.

Private Physicians

Individuals with HIV/AIDS may receive care from an HIV specialist, family practitioner, general practitioner, and internist, as well as specialists in internal medicine or infectious diseases. While some types of physicians will maintain regular contact with surveillance personnel, all physicians should know how to identify and report cases of HIV/AIDS.

Reportable Events

Reportable events span the spectrum of HIV disease, from the first confirmed HIV-positive test result to death. After a case has been reported, updates to HIV/AIDS case reports are generally submitted to the Surveillance Section when the following sentinel events occur:

- the CD4+ T-lymphocyte count of an HIV-infected case drops below 200 or 14 percent;
- an HIV-infected case is diagnosed with any opportunistic infection, which requires the reporting of diagnosis date and category (presumptive or definitive);
- an HIV-infected case becomes pregnant or delivers a live infant; or
- an HIV-infected case dies.

Health care providers use viral load and CD4+ T-lymphocyte testing to monitor the infection and guide treatment decisions for patients with HIV. A viral load measures the amount of virus in blood plasma or other tissues. Viral load tests are performed on samples from HIV-infected people as part of medical care to determine prognosis and treatment of HIV. Because the HIV reporting system is laboratory-driven, all viral loads are required to be reported to LHJs. Therefore, LHJs will often receive multiple laboratory reports for a single individual.

HIV ribonucleic acid (RNA) and CD4+ counts can serve as a surrogate marker of HIV disease progression. Therefore, once the surveillance case definition for HIV or AIDS has been met, it is important to include laboratory tests coincident with other sentinel events, such as the diagnosis of opportunistic infections or death.

III. Pediatric Surveillance

CDC case definitions for pediatric HIV and AIDS apply to children under the age of 13 years. Complete pediatric HIV/AIDS case reporting requires more than the demographic and clinical data provided for adult and adolescent cases. HIV/AIDS cases involving mother-to-child transmission generally include the child's neonatal status (full-term, premature), any preventive antiretroviral drug therapy, and other information related to each child's birth. Mother-to-child infection is the most common route of transmission of HIV in pediatric cases. An HIV-infected mother can transmit HIV to her child *in utero* through transplacental infection; during birth and delivery through exposure to maternal blood; and during breastfeeding. Maternal risk information plays a critical role in prevention planning and service delivery strategies.

Pediatric HIV

The HIV and AIDS case definitions are different for children than for adults. Because children receive maternal HIV antibodies that can be detected as long as 18 months after birth, HIV antibody tests, such as the enzyme-linked immunosorbent assay, cannot be used to detect HIV. In children under 18 months of age, an HIV deoxyribonucleic acid (DNA) test, such as the HIV DNA polymerase chain reaction (DNA PCR), P24 Antigen, viral culture, or viral load is used instead. After 18 months of age, HIV antibody tests are considered highly reliable and HIV infection can be diagnosed on the basis of repeated positive HIV antibody tests and a confirmatory test such as Western blot (Wb).

Pediatric AIDS

Although the CD4+ count is clinically useful, a low CD4+ count is not an AIDS-defining condition for pediatric cases. CD4+ cell counts in HIV-infected children are dependent on age, so a CD4+ test result, which is often used to diagnose AIDS in adults and adolescents, is interpreted differently for children.

Special Considerations for Pediatric Cases

In addition to opportunistic infections associated with AIDS in adults and adolescents, children with AIDS can develop severe forms of common childhood bacterial infections. These include otitis media (ear infections), tonsillitis, and conjunctivitis or "pink eye," and are not considered AIDS-defining. Superficial skin or mucosal abscesses and indwelling catheter-related infections are also excluded from AIDS defining conditions.

Candidiasis, or thrush, is a fungal infection commonly found in infants and adults. Esophageal candidiasis, which infects the throat and windpipe, and candidiasis in the lungs are AIDS-defining condition for both children and adults. Oral candidiasis alone is common among infants and adults and is not sufficient basis for an AIDS diagnosis.

Wasting syndrome is another AIDS-defining condition for both children and adults. Wasting syndrome is not the same as "failure to thrive." A diagnosis of wasting syndrome includes persistent weight loss, plus chronic diarrhea or documented fever in the absence of other opportunistic infections that cause these symptoms or medical treatment that causes diarrhea and weight loss.

IV. Death Ascertainment

At the local level, there are three main sources of data on deaths of individuals with HIV/AIDS:

- reviews of local death certificates;
- contacts with health care providers; and
- medical record reviews.

Death ascertainment efforts are limited, however, when an HIV-infected individual relocates to another LHJ. Death information from providers and local death certificates may contain inaccuracies that are corrected after death data has been received by CDPH's Office of Vital Records, or deaths may simply not be reliably reported.

To address these limitations, OA links statewide HIV case records with death records from CDPH's Office of Vital Records and with national death registries. Updated death information and any potentially unreported cases discovered in this process are provided to LHJs so that updates can be made to the local and state datasets. To assist LHJs in obtaining death data suitable for analysis and to ensure accuracy of death information in the statewide HIV/AIDS surveillance dataset, the Surveillance Section provides the underlying and contributing cause of death, coded using rules established by the World Health Organization and consistent with the International Classification of Diseases and Related Health Problems (ICD).

This activity provides LHJs with death information for persons with HIV/AIDS who have moved to another jurisdiction within California and helps correct inaccurate data obtained from the original death certificates. Any discrepancy between the death certificate record and the HIV/AIDS case report should be investigated.

Death Certificate Only (DCO) Cases

Using death records for HIV/AIDS case finding involves matching all death certificate records that mention HIV infection in the underlying or contributing causes of death to reported HIV cases. Death certificate records that only mention an AIDS-defining condition may also be used to identify unreported cases. However, investigation of death certificates that only mention conditions such as candidiasis, which are generally related to immunosuppression, but can be caused by other diseases such as cervical cancer, may yield few unreported cases.

Laboratory confirmation of HIV is required to meet CDC's AIDS case definition for several AIDS-defining opportunistic infections. Therefore, an AIDS-defining condition alone is insufficient for confirmation of HIV infection. OA and CDC discourage against the use of physician documentation, death certificates, ICD-10 codes, or other indicators of HIV infection, absent a confirmatory laboratory test, as the sole basis for the HIV diagnosis date for AIDS case reports.

V. Security and Confidentiality

Chapter Summary

Assuring the confidentiality of eHARS data helps to maximize the public health benefits of surveillance. Violations of confidentiality can expose HIV-positive individuals to serious harm and undermine the acceptability of the reporting system. For the purposes of this document, the term, “confidentiality,” refers to the protection of private information about individuals from disclosure in any identifying manner, except as permitted by law. Based on the description of breaches and activities described in Volume III of the CDC/CSTE Technical Guidance, for the purposes of this document, “disclosure” or “disclose” means to release, divulge, or otherwise communicate all or part of any confidential record either verbally, in writing, or using electronic methods; a disclosure may be authorized in some circumstances and strictly prohibited in others. Both state and federal laws expressly define the confidential nature of public health records, and the conditions under which disclosures may occur. As a result, CDC has established standards for security and confidentiality to protect HIV/AIDS case information. The Surveillance Section must comply with national HIV/AIDS program standards as a condition of funding for HIV/AIDS surveillance. Based on the activities described in Volume III of the CDC/CSTE Technical Guidance and activities described in the CDPH Health Administrative Manual, the term “security” is used to describe the means by which confidential information is safeguarded from improper use or disclosure.

OA has long-established security measures in place to safeguard HIV/AIDS public health records from both internal and external threats to privacy and data integrity. These measures integrate best-practice methods for maintaining data security, and serve as a model for LHJs to guide local practices. The Surveillance Section also provides technical assistance and support to LHJs in promoting vigorous security and confidentiality practices for statewide HIV/AIDS surveillance operations. These protections are both in conformity with statutory confidentiality provisions and CDC guidelines. For example, CDC PRs state that HIV/AIDS surveillance information must be maintained in a physically secure environment. According to CDC guidelines, electronic data must be held in a technologically secure environment, minimizing the number of staff with access to confidential data, and restricting the number locations where confidential data are maintained. Once electronic data are no longer needed, they must be sanitized prior to disposal in accordance with the CDC guidelines. Each staff member ultimately has a legal and ethical obligation to protect the confidentiality of HIV/AIDS case reports and any identifying patient information collected, accessed, or maintained in the course of surveillance activities. The CDC Security and Confidentiality Guide can be found at: <http://www.cdc.gov/nchhstp/programintegration/docs/PCSIDataSecurityGuidelines.pdf>.

VI. National HIV/AIDS Program Standards

As a federal cooperative agreement grantee, the Surveillance Section must comply with the requirements established by CDC for HIV/AIDS surveillance. These requirements, which represent the minimum standard for security and confidentiality, apply to all state and LHJ staff and contractors funded through CDC to perform HIV/AIDS surveillance. The ORP must annually certify that all CDC standards for security and confidentiality have been met and, in some cases, CDC PRs call for ORP to establish specific measures that operationalize CDC security standards.

CDC guidelines for HIV/AIDS surveillance also encompass a set of security considerations. Unlike PRs, these security considerations are CDC recommendations and represent best practices for the protection of HIV/AIDS surveillance information. The ten guiding principles are:

- Public health data should be acquired, used, disclosed, and stored for legitimate public health purposes.
- Programs should collect the minimum amount of personally identifiable information necessary to conduct public health activities.
- Programs should have strong policies to protect the privacy and security of personally identifiable data.
- Data collection and use policies should reflect respect for the rights of individuals and community groups and minimize undue burden.
- Programs should have policies and procedures to ensure the quality of any data they collect or use.
- Programs have the obligation to use and disseminate summary data to relevant stakeholders in a timely manner.
- Programs should share data for legitimate public health purposes and may establish data-use agreements to facilitate sharing data in a timely manner.
- Public health data should be maintained in a secure environment and transmitted through secure methods.
- The number of persons and entities granted access to identifiable data should be minimized.
- Program officials should be active, responsible stewards of public health data.

VII. Federal and State Statutes or Regulations

Both state and federal laws and regulations protect the confidentiality of HIV/AIDS public health records. While assuring the privacy of individuals is both a legal and ethical obligation, it is also imperative because such violations may lead to considerable harm. The potential adverse outcomes include stigmatization, discrimination, loss of employment, denial of insurance, physical harm, eviction, and the rejection of family and friends. Moreover, wrongful disclosures give cause for legal proceedings alleging infringement of statutory confidentiality protection, discrimination, invasion of privacy, and/or intentional or negligent infliction of emotional distress.

Federal Protections

Various federal statutes, regulations, and case laws provide legal protection of HIV/AIDS surveillance information. These safeguards include a right to informational privacy under the Fifth and Fourteenth Amendments of the Constitution. The Freedom of Information Act of 1966 (specifically United States Code Section 552(b)[6]) and the Privacy Act of 1974 provide additional protections. 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. For a copy of the CDC Assurance of Confidentiality Statement refer to the Technical Guidance for HIV/AIDS Surveillance Programs, Volume III: Security and Confidentiality Guidelines. To protect the privacy of persons with HIV/AIDS, local and state surveillance program staff does not send names or other specific identifying information to CDC.

State Protections

HSC Section 121035

All HIV/AIDS case reports and any information collected or maintained in the course of HIV/AIDS surveillance activities that may directly or indirectly identify an individual are considered confidential public health records under HSC Section 121035. Confidential public health records relating to HIV/AIDS cases, as defined under HSC Section 121035 refer to any paper or electronic records maintained by OA, LHJs, or agency, or its agent, which identifies personal information. This personal information includes but is not limited to, name, Social Security Number, address, employer, or other information that may directly or indirectly lead to the identification (ID) of the individual who is the subject of the record. This definition applies to data in eHARS. It also applies to any directly or indirectly identifying information associated with the collection, investigation, or monitoring of case information by the Surveillance Section or LHJs.

Materials that contain personally identifying information include but are not limited to the following: all completed ACRFs, supplemental materials used for surveillance purposes such as laboratory reports, death certificates, medical record review notes, follow-up materials for investigations of Cases of Public Health Importance (COPHI) or No Identified Risk (NIR), and surveillance investigation notes. In addition to protecting paper documents and electronic files, information communicated orally should also be treated with the utmost confidentiality, regardless of whether such information has been incorporated into the surveillance system.

HSC Section 121025

HSC Section 121025 requires that state and local health agencies maintain the confidentiality of HIV/AIDS-related public health records. Any personally identifying information in these public health records must remain confidential and cannot be disclosed without written authorization from the person named in the record, or his or her guardian or conservator, except for public health purposes as provided under the law [HSC Section 121025(a)]. Pursuant to HSC Section 121025(b), personally identifying information in public health records may be disclosed by state or local health agencies to other local, state, or federal public health agencies that need the information to carry out their duties in the investigation, control, or surveillance of disease.

Furthermore, any disclosure of public health records that is permitted under the law must be limited to only the information necessary for the purpose of that disclosure, and must be protected from any further disclosure [HSC Section 121025(c)]. Because public health agencies may only disclose HIV/AIDS public health records to the extent permitted by law, agencies should avoid releasing confidential information for the purpose of case management, referrals to other services, or for any other purpose unless expressly authorized by law. The HIV/AIDS surveillance system is not designed for either case management purposes or referral services. The provision of such services are generally achieved through strategies and programs designed for the purposes of HIV prevention and treatment.

Fines and Penalties for Unauthorized Disclosures

Except as permitted by law, any person who negligently discloses information contained in a confidential public health record to a third party is subject to a civil penalty of up to \$5,000 plus court costs, as provided in HSC Section 121025(e)(1). Any person who willfully or maliciously discloses the content of a public health record, except as authorized by law, is subject to a civil penalty of \$5,000-\$50,000 plus court costs as provided by HSC Section 121025(e)(2).

Any willful, malicious, or negligent disclosure of information contained in a public health record in violation of state law that results in economic, bodily, or psychological harm to the person named in the record is a misdemeanor, punishable by imprisonment for a period of up to one year and/or a fine of up to \$50,000 plus court costs [HSC Section 121025(e)(3)].

Any person who is guilty of a confidentiality infringement of the type mentioned above may be sued by the injured party and shall be personally liable for all actual damages incurred for economic, bodily, or psychological harm as a result of the breach [HSC Section 121025(e)(4)]. Each disclosure in violation of California law is a separate, actionable offense [HSC Section 121025(e)(5)].

VIII. Surveillance Activities

Compliance with National Standards

CDC funding for state and local HIV/AIDS surveillance is contingent upon the agency's ability to ensure the physical and electronic security of HIV/AIDS case information. In compliance with the terms of the federal cooperative agreement, ORP must annually certify that all PRs have been met. This certification requires an ongoing review of security practices at the Surveillance Section and at all reporting sites in the state.

At the State level, under the direction of the ORP, the Surveillance Section conducts an annual review of security practices using CDC's Security and Confidentiality PR Checklist. This process is intended to enhance existing protections in response to new surveillance activities, operational changes, and evolving information technologies. The checklist is also suitable for LHJ's efforts to evaluate local practices in view of the national program standards. Furthermore, as part of a program review performed at least annually, the Surveillance Section surveillance coordinators review security and confidentiality practices at each LHJ.

During the program review, the surveillance coordinators assess local compliance with CDC PRs. This activity includes, but is not limited to, a review of confidentiality agreements, physical security measures, security software, confidentiality practices, destruction of information, and secure mail procedures. The surveillance coordinators document both areas of strength and areas that need improvement. Upon request, surveillance staff also provide assistance to LHJs in enhancing local security measures to meet the national PRs. To avoid gaps in communication between the Surveillance Section and LHJs, LHJs are encouraged to immediately notify their assigned coordinators when a new staff person has been hired. This notification also allows the Surveillance Section to monitor confidentiality agreements and ensure that staff training takes place in a timely manner.

Staff Responsibilities

For the purposes of this chapter, 'staff' refers to both state and LHJ personnel, unless otherwise specified. All HIV/AIDS surveillance staff, including information technology (IT) employees and contractors, who require access to confidential public health records to carry out assigned duties must sign a Confidentiality Agreement (CDPH 8689 [10/12]) pursuant to HSC Section 121022 (e). Under state law, authorized department staff must sign a Confidentiality Agreement prior to accessing confidential HIV-related public health records [HSC Section 121022 (e)]. It is required that confidentiality agreements be signed at the time of employment and every 12 months thereafter.

Individuals are not authorized to access confidential surveillance information until the signed confidentiality agreements have been reviewed and signed by the Chief of the Surveillance Section or his/her designee. Additionally, no staff member may be assigned or possess any keys, passwords, codes, or electronic key cards that would permit access to confidential surveillance information until such authorization has been granted and verified. The Surveillance Section will retain the original signed confidentiality agreement on file; the LHJ's HIV/AIDS surveillance programs should maintain a copy of all signed agreements, and program staff should be provided a copy of their signed agreement for their own records. Additionally, CDC guidelines require all HIV/AIDS surveillance staff, including IT staff and contractors, to annually receive a security and confidentiality training, the date of which must be documented in the individual's personnel file.

It is essential that all HIV/AIDS surveillance staff have knowledge about, and immediate access to, any written documentation on security and confidentiality provided by their department. Additionally, each individual is responsible for carefully attending to security irregularities and immediately reporting suspected breaches in accordance with the Confidentiality Agreement [CDPH 8689 (10/12)]. HSC Section 121022(g) requires the immediate investigation of any suspected confidentiality breach, and stipulates that any evidence of an actual breach must be reported to law enforcement. Surveillance programs may incorporate various strategies to continually reinforce key security practices and standards such as: including reminders of HIV/AIDS confidentiality protocols at scheduled staff meetings, displaying posters on workplace walls to highlight security and confidentiality practices, and maintaining a copy of applicable HIV/AIDS-related laws in the office.

Knowing who is authorized to have access to restricted areas and confidential case information, and challenging any persons suspected of not having the appropriate authorization, are key measures to maintaining security. Sharing of confidential HIV/AIDS surveillance information is only permitted for the purpose of carrying out official surveillance duties and in accordance with the law. This practice limits access to confidential surveillance information to only those individuals authorized and even the only on a need-to-know basis. The term, need-to-know is used by the Surveillance Section to describe a security principle that is integral to holding data and information in a secure and confidential manner. The following measures demonstrate how this principle can be applied in practice:

- Verifying an individual's identity and authority to access any HIV/AIDS surveillance information containing personal identifiers before such information is shared;
- Limiting the amount and sensitivity of information that is accessed, used, or exchanged to the minimum necessary to complete a given task; and
- Minimizing the number of times that confidential surveillance information containing personal identifiers is accessed or used.

Because HIV/AIDS cases are reported and stored by name, data handlers are encouraged to exercise extreme caution in the collection, transfer, and analysis of surveillance data and information. CDC strongly advises against the use of electronic modes of transmission such as electronic mail (email) or facsimile to transmit any case information containing names or other personally identifying information. A longstanding method of ensuring case confidentiality during the exchange of information relies on the use of Soundex, date of birth, and gender, in combination instead of the patient's name. Soundex refers to a phonetic, alphanumeric code assigned to surnames using a CDC-approved algorithm. This standard combination of

variables may be used in the course of surveillance-related activities such as checking laboratory reports or HIV/AIDS case reports against previously reported cases. In the absence of information connecting the patient to diagnosis information, the combination of Soundex, date of birth, and gender alone generally presents a minimal direct disclosure risk. However, safeguarding privacy demands that HIV/AIDS program staff consider the size of the underlying population when assessing disclosure risk in any given context.

Confidentiality in the Surveillance Unit

For the purposes of this chapter, the 'surveillance unit' refers to both state and local surveillance program offices. According to CDC guidelines, all staff members are individually responsible for protecting their own workstation, computer, or other devices associated with confidential surveillance information or data. This responsibility includes protecting any keys, passwords, codes, and electronic key cards that would allow access to confidential case information, along with protecting all restricted areas. Within the surveillance unit, the issuance of keys, passwords, or codes must be carefully monitored.

Vigilance by staff is vital to preventing the integrity of surveillance data from being compromised through damage, destruction, or by unauthorized modification. The Surveillance Section practice is to report any suspected malfunction in security software to an immediate supervisor. CDC guidelines also require that staff take reasonable measures not to infect surveillance software with computer viruses or to allow damage to hardware. Measures that help prevent such damage include not disabling or turning off any virus-checking software, and scanning all electronic media prior to use.

Under limited and controlled circumstances, unauthorized individuals, such as maintenance crews or janitorial staff, may be permitted access to the secured areas where surveillance information is maintained. If allowed access, a provision in CDC guidelines requires authorized surveillance staff to escort any unauthorized persons within the surveillance unit. If surveillance personnel are not available for escort within the secured area, CDC guidelines require that access to unauthorized individuals be granted under certain strict security conditions specified in a local plan and approved by ORP. Because California law protects the confidentiality of HIV/AIDS public health records, staff should avoid allowing any unauthorized persons to overhear or observe any information associated with confidential HIV/AIDS case information while accessing the secured area. To protect confidential information, the Surveillance Section staff are not to leave their workstation unattended with confidential case information visible on their computer monitor. Staff can secure their workstation before leaving it unattended by locking their computers using a password or shutting down the system (e.g., for breaks, meetings, or at the end of the work day). Within the workstation, any paper documents having personal identifying information must be stored in a locked file cabinet.

Additionally, CDC guidelines require that all unencrypted external storage media containing confidential surveillance information be locked away when not in use. It is also important that printouts with personal identifiers be retrieved from the printer immediately. Before disposal, staff must shred documents containing confidential HIV/AIDS-related information using a commercial quality shredder with cross-cutting capability, in accordance with CDC guidelines.

Confidentiality in the Provider Setting

In the course of surveillance activities, staff may conduct medical record reviews of HIV/AIDS-related information at hospitals, clinics, private medical offices, or in non-clinical settings where confidential patient information is maintained. Protecting confidentiality requires that staff conduct such record reviews in restricted areas to ensure that confidential materials remain secure at all times. Case confidentiality is enhanced when reporting entities assign certain personnel the responsibility of reporting HIV/AIDS cases and communicating with the local surveillance program. For example, this practice limits the number of staff in provider settings that need access to HIV/AIDS-related data. Furthermore, this practice restricts the handling of information to certain staff with knowledge about the special security considerations required for HIV/AIDS case information.

Communications

Secure communication relies foremost on the conduct of surveillance staff. The objective of secure communication is to avoid situations that allow unauthorized persons to overhear any confidential information. OA does not permit staff to discuss or divulge any confidential surveillance information in the presence of unauthorized persons or outside of the workplace. For example, staff must maintain case confidentiality by only conducting verbal conversations that identify cases using names or other personal identifiers in secured areas where no unauthorized persons may overhear.

In particular, ensuring confidentiality requires that staff conduct all confidential telephone conversations using phones that are connected to landlines. Cordless telephones and wireless communication are not considered secure means of conveying confidential information. Verifying the identity of the other persons when initiating or receiving telephone calls discussing HIV/AIDS case information is vital to protecting individual privacy. If the authorization of any individual to receive confidential information is not verifiable, the Surveillance Section will not provide information to that individual, as any release of confidential information in this context would risk violating an individual's confidentiality. In this case, staff could prevent an unauthorized disclosure by contacting the appropriate person in the agency to verify the caller's identity and authorization to access specific HIV/AIDS case information.

When making or responding to requests for information about possible HIV/AIDS cases in another LHJ, surveillance staff should consider whether the release of information is in compliance with state law. To protect the confidentiality of statewide HIV/AIDS data, out-of-state communication regarding HIV/AIDS case reports is only conducted at the state level between surveillance staff authorized on the CSTE contact list.

Communication during Special Investigations

During a NIR investigations or interviews, surveillance staff should not leave voice messages, provide business cards, or send letters to the residence of an HIV-infected individual that include any terms associated with HIV/AIDS or the health department, in accordance with CDC guidelines. This practice is necessary to prevent the inadvertent disclosure of an individual's HIV/AIDS status, should a family member or friend hear the message or see the materials. Information on confidential interview techniques may be obtained from CDC.

Securing Electronic Data

CDC guidelines require that analysis datasets have personal identifiers removed if taken out of the secured area or accessed from an unsecured area. In addition, any electronic data used by the surveillance program relating to HIV/AIDS case information containing personal identifiers is

considered confidential under California law, and must be protected from unauthorized disclosures. This legal protection is not specific to data stored in eHARS. For example, analysis datasets derived from eHARS, or clinical data management systems and laboratory databases used for surveillance that contain information that can directly or potentially indirectly identify an individual require the utmost protection. Databases that contain direct or indirect identifiers for HIV-infected individuals are highly confidential and require the same security standards as eHARS. According to CDC PRs, any ancillary databases or electronic files containing direct or indirect identifiers for HIV-infected individuals must be encrypted when not in use. All electronic data, whether stored on servers or removable media, must be sanitized prior to disposal to ensure confidentiality.

Access to personally-identifying information (PII) and de-identified data is limited to individuals on a need-to-know basis. Access must be approved by the employee's manager and the chief of the OA Surveillance Section. Access to eHARS is granted in the same manner, as the access level is based on the employee's classification and unit as follows:

eHARS Data Access Levels		
Staff Position	eHARS Doc. Access Level (View, Create, Modify, Delete, Import/Export)	eHARS Admin
<i>SQMU Staff</i>		
SSM I	View, Create, Modify, Delete	Yes
AHPA	View, Create, Modify, Delete	Yes
AGPA	View, Create, Modify, Delete	No
CDS	View, Create, Modify, Delete	No
SSA	View	No
OT	View	No
<i>DMAU Staff</i>		
RSS I	View, Import/Export	No
RS	View, Import/Export	No
RA II	View, Import/Export	No
HPS	View, Import/Export	No
HIS	View, Import/Export	No
Programmer	View, Import/Export	Yes
<i>Surveillance Section Staff</i>		
RSS II	View	No
RS III	View, Import/Export	No
HPS	View	No
<i>Supplemental Surveillance Section Staff</i>		
RSS I	View	No
RS	View	No
RA	View	No
<i>Other OA Staff (i.e. PRE, CRE, Etc.)</i>		
	View	No
<i>Other CDPH Staff (i.e. STD/TB/VH staff)</i>		
	View	No
<i>LHJ Staff (i.e. SF, LA, SD) *Access limited to their respective site code data only</i>		
	View, Create, Modify, Delete	Yes

Physical Security

All physical locations containing HIV/AIDS surveillance data in electronic or paper format, as well as workstations for surveillance personnel must be sequestered inside a locked, secured area with access limited to authorized personnel in accordance with CDC PRs. If the area housing surveillance data is on the first floor, any windows that open must be secured using a permanent seal, a security alarm, or other reliable method. Paper copies of surveillance information containing identifying information must be stored inside a locked file cabinet located inside a locked room. All documents containing confidential HIV/AIDS-related information must be shredded by authorized surveillance personnel using a commercial quality shredder with cross-cutting capability before disposal. According to California law, only authorized LHJ personnel who have signed a confidentiality agreement are permitted to handle confidential public health records.

Physical Security in the Surveillance Section

The Surveillance Section is housed inside in a secured, locked suite with access limited to authorized personnel. Entry into the section is controlled by an electronic key card system that is activated only by an authorized ID badge. In addition to surveillance staff, non-surveillance OA staff may be granted authorization to access the Surveillance Section in order to carry out official programmatic duties related to public health purposes, such as epidemiological monitoring. However, all non-surveillance OA staff with Surveillance Section badge access must obtain approval by the Chief of the section or ORP, and are required to complete security and confidentiality training and sign a confidentiality agreement.

This access authorization is limited to a minimum number of staff, whose approval is routinely reviewed by the surveillance Chief and may be revoked at any time. Lost or stolen ID badges are considered a serious threat to security because they provide access to restricted areas. All staff must report any lost or stolen ID badge to the security office.

Access to the Surveillance Section by individuals with non-activated ID badges, such as administrative OA personnel, janitorial staff, and building maintenance crews, must be minimized and carefully monitored. These individuals are allowed entry into the Surveillance Section only upon approval by the Chief and during predetermined times when an authorized Surveillance Section staff member is available to escort them around the premises. The Surveillance Section staff members and contractors must not allow unauthorized persons access to any computers, databases, or file cabinets used to process or store HIV/AIDS case information. Staff are individually responsible for attending to their workspace and safeguarding confidential case information on paper documents, electronic media, or visible from a computer monitor, as described in this chapter. Also, the Surveillance Section staff must strictly follow confidentiality practices to prevent any unauthorized personnel from overhearing or viewing confidential case information. Although access to the section by janitorial staff is controlled, the intent of this practice is to add an additional layer of security. Mail delivery to the section is performed by a designated Surveillance Section staff member in order to further limit the need for unauthorized staff to access the secured area. Administrative functions that involve non-surveillance OA staff are to be handled outside of the section in an appropriate location.

Physical Security outside of the Surveillance Section

Program personnel working outside of the Surveillance Section handling data or documents with personally identifying information (PII) must 1) return the documents or electronic device containing PII to a secure area by close of business 2) obtain prior approval from the program

manager for not doing so, or 3) follow approved procedures for handling these documents and data.

Documents or electronic devices that contain PII and are not returned to a secure work site by close of business must be stored in a locked file cabinet in the staff member's residence. Any PII outside of the Surveillance Section Office must be in the possession of the staff member at all times. Personnel may not leave documents or electronic devices containing PII in vehicles that are unattended. Personnel who are abstracting PII in the field may only do so in a secure environment where the PII is visible solely to authorized staff. If personnel are traveling with PII documents or electronic devices that contain PII, it must be locked in a secure suitcase kept in their possession at all times until they are able to lock PII information in a secure file cabinet in a staff member's residence or other secure worksite. Transportation of PII outside of secure work areas should be minimized and done so in a secure manner.

Some personnel are authorized by their program manager to travel with documents containing PII, because they are remote employees. Remote employees have unusual travel distances between clinics, hospitals, physician's offices, and so forth, and the Surveillance Section. Remote employees do patient interviews and chart abstractions across the state of California. Remote employees upload information they obtain from patient interviews and chart abstractions from their electronic device onto a secure website known as the Secure File Transfer (SFT) site. All documents stored on the electronic device are then deleted. After personnel contact patients to schedule interviews using a mobile phone, all contact information for the patient is then deleted from call logs. Remote employees who handle paper documents containing PII must store documents in a locked briefcase while traveling and a locked file cabinet at home. All paper documents are brought to the Surveillance Section once a year to be shredded after a project period closes.

All electronic devices and files that contain PII must be encrypted when stored on any removable media or portable device (i.e., USB thumb drives, floppies, CD/DVD, Blackberry, back-up tapes, etc.). They must be encrypted using a FIPS 140-2 certified algorithm, such as AES, with a 128 bit or higher encryption key.

IX. Movement of Confidential Materials

Confidential Mail Practices

In order to protect patient confidentiality, CDC guidelines require that the amount and level of sensitivity of information contained in any one piece of mail be kept to a minimum. In compliance with CDC requirements, data containing HIV/AIDS case information that is stored on any electronic media must be encrypted prior to mailing. The federal encryption standards required by CDC are detailed in the prior section.

For any outgoing confidential mailing, double envelopes should be used for added security. This double envelope procedure involves placing the case information (either the paper documents or encrypted electronic data) in an envelope, sealing it with tape, marking the outside "confidential," and addressing it to the specific authorized individual. This envelope is then placed inside another envelope and sealed with tape; the outer envelope will have the appropriate address and name of an authorized surveillance person. Note that the *outer* envelope does not read "confidential." No portion of the outer envelope, including the sender or

recipient address or label, may contain terms that could be associated with HIV or AIDS. Our internal policy requires the use of “traceable services” for outgoing mail that contains identifying or potentially identifying information regarding individuals with HIV. A “traceable service” is a service that issues a tracking number to each package, maintains a log of where the package is during routing, and requires that the recipient signs for the package upon delivery.

Transferring Electronic Data between State and Local Surveillance Sites

OA established a Secure File Transfer (SFT), which allows the Surveillance Section and LHJs to exchange electronic information over a secure network connection. Please see the SFT Standard Operating Procedures (SOPs) for more details (Appendix, page 74).

Most emails received and sent by the Surveillance Section are not encrypted and are not maintained on a secure network. Because email is typically not secure, email transmission of personally identifying or potentially identifying HIV/AIDS information to the Surveillance Section is not permitted. To avoid delivering confidential information into unauthorized hands, the Surveillance Section does not fax documents containing directly or indirectly identifying information regarding HIV/AIDS cases.

Transferring Data to CDC

The Surveillance Section is responsible for transferring statewide HIV/AIDS core surveillance case data directly to CDC. Before surveillance data are sent to CDC, the file is stripped of all personal identifiers (e.g., names, addresses, Social Security Numbers, or telephone numbers). The file is then encrypted and transferred to the CDC via their Secured Data Network.

X. Data Release

According to the CDC, access to and use of surveillance information or data must be defined in a data release policy. The purpose of a data release policy is to ensure the confidentiality of HIV/AIDS case information by establishing minimum standards for disclosure protection when releasing data. The data release policy guides HIV/AIDS surveillance staff, researchers, and other data users on the types of data allowed for release, who is authorized to receive the data, and for what purposes the data may be used. Additionally, it specifies standards and practices that minimize the risk of disclosing identities or other confidential information of individuals with HIV/AIDS. Any data release not covered by the data release policy must be reviewed and approved by the ORP.

In compliance with CDC guidelines, all reporting sites must restrict access to raw data or data tables that include small denominator populations and any potentially identifying information. In general, surveillance information (e.g., analysis datasets) containing individual-level data is not released, other than to staff at of the Surveillance Unit. However, the release of individual-level surveillance data for research purposes may be allowed under the following conditions: 1) there is a demonstrated need for these data; 2) a data sharing agreement specifying the rules of access and final disposition of the information is signed; and 3) the release is approved by the ORP. OA will apply the same protections for security that are specified in the national program standards to any analysis datasets extracted from the HIV/AIDS surveillance system.

XI. Security Breaches

The unauthorized release of confidential information about an individual, in any manner, constitutes a breach of confidentiality under the law, regardless of whether or not the breach was intentional. Pursuant to California law, an individual who is responsible for a breach of confidentiality is subject to civil and/or criminal penalties, depending on the nature of the violation. OA, LHJ staff, and contractors who are authorized to access surveillance data are responsible for reporting any suspected confidentiality breach, in accordance with the terms and conditions of the Confidentiality Agreement (CDPH 8689 [10/12]). A confidentiality breach refers to a security infraction resulting in the release of private information about an individual with or without harm to one or more individuals. A security breach may occur whenever security measures are compromised or circumvented, either intentionally or unintentionally.

A breach of confidentiality must be immediately investigated to assess causes and implement corrective action. In the event that a breach of confidentiality is suspected or has occurred, the Surveillance Section staff must immediately notify the Chief. If a breach of confidentiality has occurred at the city or county level, LHJ should immediately notify the AIDS director who will inform the local health officer and the Surveillance Section Chief. When LHJs suspect that a breach may have occurred, the local health officer, in accordance with HSC Section 121022 (g)(1), will promptly investigate the suspected or actual breach in conjunction with OA. Any evidence of an actual breach of confidentiality of an HIV-related public health record will be reported to the proper law enforcement agency, as required by law.

In compliance with CDC cooperative agreement, a breach that results in the release of private information about one or more individuals must be reported immediately to the team leader of the Reporting, Analysis, and Evaluation Team, HICSB, DHAP, NCHSTP. Breaches that do not result in the unauthorized release of private information are not reported to CDC but rather are handled by the state or local surveillance program. Under these circumstances, the security of the surveillance system may have been breached without resulting in the disclosure of private information and harm to any individual(s). Any suspected breach in security should be reported to the Surveillance Section Chief.

Attention should be paid to identifying a breach, immediately responding to it, and containing any resulting damage. Subsequently, it is important to identify lessons learned from the event, and if necessary, revise or enhance confidentiality practices, and upgrade physical or operational security measures. The supervising program personnel are encouraged to:

- develop an immediate response and take appropriate action preventing any further disclosure of the information;
- complete a summary of the nature of the breach and a resolution; and
- prepare a step-by-step plan to revise current security and confidentiality practices and prevent additional breaches in confidentiality.

XII. Special Investigations

Chapter Summary

Accurate risk factor ascertainment and documentation is an important part of identifying populations most in need of state and federal funding for HIV prevention efforts. Risk factor ascertainment is a term used throughout this chapter to describe the gathering of information about risk factors for HIV infection. The term 'risk factor' is used to denote specific routes of potential exposure to HIV. Risk factors are the collective term for the individual routes of exposure/transmission on which data are routinely collected for surveillance of HIV/AIDS

cases and recorded as “yes,” “no,” or “unknown” on the HIV/AIDS Case Report Form. Examples of transmission routes include sexual contact with an HIV-positive individual, or the sharing of syringes with an HIV-infected person for injection drug use. The objective of risk factor ascertainment is to identify all known risk factors that were present before an individual was diagnosed with HIV.

HIV/AIDS cases without risk information fall into three categories: No Reported Risk (NRR) Factor, No Identified Risk (NIR), and Cases of Public Health Importance (COPHI). This chapter provides an overview of COPHI and risk factor ascertainment.

The activities described in this chapter include but are not limited to:

- Process and outcome standards for risk factor ascertainment;
- Process and outcome standards for COPHI;
- Investigation and case follow up; and
- Education and training of surveillance staff.

National HIV/AIDS Program Standards

Under the federal cooperative agreement for HIV/AIDS surveillance, OA is required to report cases of public health importance to CDC. Additionally, OA must conduct COPHI investigations according to Protocol 776, which is found in the *CDC Technical Guidance for HIV/AIDS Surveillance Programs*. As a cooperative agreement grantee, OA is responsible for ensuring that statewide surveillance operations meet CDC performance standards for completeness of risk factor information.

All federally funded HIV/AIDS surveillance programs are required to have documented risk factor information for at least 85 percent of reported HIV/AIDS cases subsequent to complete case follow up. CDC has also established both process and outcome standards for COPHI and risk factor ascertainment. When achieved, these standards will assist programs in meeting the minimum performance standards for complete, accurate, and timely surveillance data. Process standards refer to specific activities that are either recommended or required to achieve certain objectives. Outcome standards refer to objectives that surveillance programs are able to measure. This section provides an overview of risk factor ascertainment and COPHI, followed by a description of process and outcome standards for each respective activity.

CDC Outcome Standards for COPHI

Based on CDC outcome standard for COPHI, OA prepares annual progress reports 12 months following each reporting year. This report lists all cases of public health importance from the previous reporting year and includes the status of each case along with the following:

- Number of cases reported;
- Number of cases where investigation was initiated;
- Number of cases with a final disposition or status;
- Number of CDC-confirmed cases (if any); and
- Percentage of cases still open (number of cases reported minus the number of cases with a final disposition/number of cases reported).

CDC Process Standards for COPHI

OA, in consultation with CDC, coordinates COPHI investigations statewide while ensuring compliance with national process standards. LHJ staff cooperates with OA to conduct COPHI

investigations and provides assistance in order to meet these objectives.

- OA and LHJs should have documentation describing their legal authority to investigate HIV cases of public health importance regardless of reporting method.
- All HIV and AIDS cases of public health importance must be investigated to confirm the reported exposure. There is no CDC minimum performance standard.
- Investigation of cases should be initiated within 3 months of date of initial case report or at the time of notification from the patient or provider, if sooner.
- A COPHI risk factor for a case can only be called confirmed by CDC in consultation with OA, after an investigation, based on criteria as outlined in Protocol 776.
- All cases should either be in 'active' investigation status or 'closed' with a final disposition.
- Cases should be closed after 1 year if no further information becomes available, but can be reopened to confirm risk factors at a later date.
- The Surveillance Section should run reports of all non-confirmed COPHI on at least a quarterly or more frequent basis depending on morbidity, using case data from the HIV/AIDS surveillance system or equivalent software that is reported to CDC.

XIII. Statutes and Regulations

Provisions of the California HSC establish the legal authority of public health agencies to investigate the nature of HIV exposures. Under HSC Section 120125, CDPH is required to examine the causes of communicable diseases occurring or likely to occur in California. Upon being informed by a health officer of any contagious, infectious, or communicable disease, CDPH is authorized to take necessary measures to ascertain the nature of the disease and prevent its spread (HSC Section 120140).

Risk factor information is routinely collected and documented using OA's Confidential HIV/AIDS Case Report Forms (CDPH 8641A and CDPH 8641P) for adult/adolescent and pediatric cases, respectively.

XIV. COPHI Cases Overview

COPHI cases occur when rare or unusual modes of HIV transmission cannot be ruled out or when there is an unusual occurrence of HIV. Examples of COPHI include cases of variant strains of HIV, cases of occupational exposure, and transmission via blood transfusion or transplantation surgery.

A priority for HIV/AIDS surveillance, COPHI investigations provide findings that contribute to more effective public health practices. For example, data about occupational HIV exposures may be used to develop better strategies to prevent HIV transmission in certain occupational settings.

In accordance with CDC guidelines for HIV/AIDS surveillance, OA must report suspected occurrences of COPHI. When COPHI is suspected, LHJs are responsible for notifying OA, which in turn notifies CDC about such reports. CDC, in consultation with OA, will determine whether a case meets COPHI classification. All federally funded HIV/AIDS surveillance programs must conduct COPHI investigations in accordance with Protocol 776 established by CDC.

NRR Cases

CDC classification, NRR, applies to cases reported without any risk factor information, or with unconfirmed COPHI risk factor information.

NIR Cases

NRR cases are reclassified as NIR when: 1) all available data sources have been reviewed or contacted; and 2) 1 year has elapsed since the date of the initial case report regardless of whether or not case follow up was initiated or completed.

Identifying Cases for Follow Up

To be consistent with CDC guidelines, risk factor ascertainment is initiated when an LHJ receives any initial case reports of potential HIV/AIDS cases lacking risk factor information.

COPHI Case Investigation

COPHI investigations should only be undertaken by staff persons who have been trained to perform these activities and who possess an adequate level of expertise in HIV/AIDS surveillance. At the state level, OA designates a surveillance coordinator to provide technical assistance to LHJ staff and carry out investigations regarding a potential COPHI. Every LHJ is encouraged to designate a trained staff person as the coordinator for follow-up investigations who will work in conjunction with OA.

LHJs should immediately notify the Surveillance Section regarding a potential COPHI. OA's COPHI coordinator will review the information and, as appropriate, forward the case to CDC's COPHI coordinator. The designated OA surveillance coordinator will immediately contact the COPHI coordinator in HICSB of CDC for a suspected COPHI case. OA, in consultation with CDC, will determine whether a case meets the COPHI classification.

COPHI Case Criteria

In order for a case to be considered COPHI, it must meet at least one of the following criteria established by CDC:

- Clusters of unusual clinical, laboratory, or geographic occurrences that have potential public health significance.
- Possible unusual transmission circumstances where scientific evidence can confirm or refute the possibility of transmission (where possible).
- Cases without detectable antibody response on standard testing.
- Cases of HIV-2 and non-B subtypes in the United States.
- Infections in children (under 13 years of age) not attributed to perinatal mother-to-child exposure.

Prioritizing Risk Factor Ascertainment Activities

CDC has established a hierarchy of investigations, which ensures timely reporting of cases of public health importance. Based on CDC guidelines, the first priority for LHJs is to follow up on COPHI, followed by NRR cases, and cases with incomplete risk factor information. Follow up on cases with no reported risk factors should be prioritized based on the volume of NRR cases in each facility.

XV. HIV/AIDS Case Procession

Who Reports Laboratory Tests

The laboratory director or authorized designee must report confirmed HIV tests within 7 calendar days to the local jurisdiction where the health care provider facility is located (CCR, Title 17, Section 2643.10).

Some laboratories refer specimens to other laboratories for testing. A reference laboratory is a laboratory that receives a specimen from another laboratory and performs one or more tests. If a laboratory sends a biological specimen to another laboratory for testing, the laboratory that first receives the specimen from the health care provider is also responsible for reporting positive results to LHJs. That is, both the initial laboratory that received the specimen and the laboratory that conducts the confirmed HIV test must report to the LHJ where the ordering health care provider is located. In cases where a California laboratory receives a biological specimen from an out-of-state laboratory or health care provider, the director of the California laboratory is responsible for reporting confirmed positive HIV test results to the appropriate state health department.

Information Reported by Laboratories

When ordering an HIV test, health care providers must provide certain patient information to the laboratory along with the specimen, such as name, birth, and gender (CCR, Title 17, Section 2643.5). Health care providers also provide the laboratory with the date the biological specimen was collected and the name, address, and phone number of the health care provider and facility that submitted the specimen to the laboratory.

The laboratory must obtain this information from the health care provider before it can report confirmed positive HIV tests to LHJs (CCR, Title 17, Section 2643.10). If any of the required information is missing, the laboratory is obligated to contact the health care provider to obtain the missing information. If the laboratory is unable to obtain the required information from the health care provider, the laboratory may find it useful to contact LHJ to assist in follow up.

Upon confirmation of HIV-positive test results, the laboratories are required to send specific information to the LHJ for each patient (CCR, Title 17, Section 2643.10). In addition to the above list of information received from the health care provider, laboratories must also report:

- the laboratory report number (also called the accession number) assigned by the laboratory;
- results of the test performed;
- date the biological specimen was tested; and
- the laboratory's Clinical Laboratory Improvement Act (CLIA) number.

If a laboratory transfers the specimen to another laboratory for testing, it may not know the date the specimen was tested at the reference laboratory. If possible, the laboratory should obtain the date from the reference laboratory. In cases where the laboratory cannot obtain the specimen test date, the date on which the test result was released to the health care provider by the laboratory that first received the specimen is conventionally provided to LHJs.

Laboratory Reporting and Incidence Surveillance

The goal of HIV incidence surveillance is to measure the number of new HIV infections per year in the California by applying the Serologic Testing Algorithm for Recent HIV Seroconversion (STARHS) Bio-Rad 1/2 plus O assay (Avidity) to residual HIV diagnostic serum specimens.

Population-based incidence estimates require the matching of an HIV diagnostic specimen to a reported HIV/AIDS case using the laboratory accession number, C&T client ID number, or other available identifiers. Therefore, it is important that laboratory reports contain the accession or C&T numbers and that this information is included in HIV/AIDS surveillance case data.

XVI. Matching HIV/AIDS Reports

LHJ staff must match incoming reports of HIV and AIDS many times during the reporting process. This is because routine laboratory testing of blood samples is a standard part of HIV health care. Laboratory tests, such as viral loads, are used to assess HIV disease progression and monitor the health of the patient's immune system. Laboratories are required by law to report all confirmed HIV tests to LHJs, regardless of whether or not the laboratory has previously submitted a report for the patient. Therefore, after the initial HIV/AIDS case has been reported, LHJs may continue to receive laboratory-initiated tests for a single individual.

However, only unduplicated HIV/AIDS cases can be submitted to CDC. To ensure LHJs only report unduplicated HIV/AIDS cases to OA, LHJ staff check incoming HIV/AIDS case reports to see if the case has been previously reported in their own jurisdiction or in another health jurisdiction in the state.

Although it happens less frequently, multiple HIV/AIDS case reports for the same case can also be reported to LHJs from health care providers. When an individual changes health care providers, the provider, complying with reporting regulations, may report an HIV or AIDS case again. Comparing information from incoming HIV/AIDS reports to previously reported cases is commonly called "case checking." Although most case checking involves laboratory reports, the process is the same for case reports received from any reporting source.

Matching to HIV/AIDS Cases Reported in LHJs

The first step in processing a confirmed HIV-positive test result from a laboratory is to match the laboratory report to previously reported HIV and AIDS case reports in LHJs. LHJ staff may compare incoming case reports to HIV/AIDS case reports received from health care providers in their jurisdiction using the patient's name, Social Security Number, birth date, and other identifying information. Useful fields that can help distinguish between records at LHJs include the patient's name (or last name, Soundex, race, ethnicity), Social Security Number (full or partial), date of birth, date of death, and provider or laboratory name. Because identifiers such as name, date of birth, and Social Security Numbers are not error free, it is important to consider both exact and inexact matches. For female patients, check the first name and date of birth with Social Security Number; females may have changed their last name for many reasons.

At the national level, CDC uses the combination of Soundex, date of birth, and sex to identify potential duplicate cases. Therefore, to assist in statewide and nationwide de-duplication efforts, it is important that LHJ surveillance staff confirm that HIV and AIDS cases with the same Soundex, date of birth, and sex represent unique individuals.

XVII. Case Checks

Once LHJs determine that an incoming HIV/AIDS case has not been previously reported in their

jurisdiction, to avoid duplication, LHJ HIV/AIDS surveillance staff must then verify that the HIV/AIDS case has not already been reported from elsewhere in California. This is because individuals can relocate many times throughout the course of their illness and health care providers and laboratories, complying with reporting regulations, may report HIV or AIDS cases for persons already in the HIV/AIDS surveillance system. Since reportable events span the spectrum of HIV disease, it is not uncommon for an individual's case information to be reported from more than one of California's 61 LHJs.

Case Checking by Phone and Electronically

It is possible to process small numbers of case checks over the phone but it is our policy that LHJ's follow the Electronic Case Check SOP (see Appendix Section, page 43). This SOP was put into place due to the extensive amount of time required to conduct case checks via phone.

XVIII. Processing Laboratory Reports

Please follow the LDET SOP available on our web site.

XIX. HIV/AIDS Case Reporting

CDC funds HIV/AIDS surveillance activities in the United States and all funded HIV/AIDS surveillance programs report HIV/AIDS cases using standardized case reporting forms. In California, cases of HIV and AIDS are reported on one of two forms (CDPH 8641A or CDPH 8641P; 'A' means Adult and 'P' means Pediatric).

The HIV/AIDS Case Report Form used to report HIV is also required for reporting an AIDS case at the time of AIDS diagnosis. The forms used for HIV and AIDS reporting in California are the green Adult HIV/AIDS Case Report Form (CDPH 8641A) and the gold Pediatric HIV/AIDS Case Report Form (CDPH 8641P). These forms are available on the OA website at: <http://www.cdph.ca.gov/pubsforms/forms/CtrIdForms/cdph8641a.pdf> so LHJs can make copies for their local health care providers.

Information Reported on HIV/AIDS Case Report Forms

The forms capture data used to describe the burden of HIV/AIDS and information used to evaluate the performance of the HIV/AIDS surveillance system. Patient identifying information, such as name and Social Security Number, is recorded on the form, but is not transmitted to CDC.

Reporting Adult/Adolescent HIV/AIDS Cases

The appropriate case report form is determined using the patient's age at HIV/AIDS diagnosis. The Adult HIV/AIDS Case Report Form is used to report HIV infections and AIDS diagnoses for adults and adolescents age 13 years or older at the time of diagnosis. The laboratory data and other requested information is consistent with CDC's case definition.

Reporting Pediatric HIV/AIDS Cases

The Pediatric HIV/AIDS Case Report Form is used to report HIV infections and AIDS diagnoses for children age 12 and under at the time of diagnosis. The laboratory data and other requested information is consistent with CDC's case definition.

Completing HIV/AIDS Case Report Forms

HIV/AIDS Case Report Forms originate at the health care provider's office once a new HIV or AIDS diagnosis is made. Often, a health care provider will designate a staff person to complete the HIV/AIDS Case Report Form. LHJ staff may also assist local health care providers with completion of the HIV/AIDS Case Report Form.

To make completion of the HIV/AIDS Case Report Form as efficient and accurate as possible, OA recommends that LHJs contact their local health care providers and provide information on how to fill out the HIV/AIDS Case Report Forms. HIV/AIDS Case Report Forms are confidential and must be sent via traceable mail or via the SFT server (CCR, Title 17, Section 2643.5).

Documenting Risk

One important aspect of quality control is to monitor NRR and NIR cases. Visual editing or proofreading of all hard copy or electronic case reports prior to sending them to OA is an important part of the quality control process. In some cases, when the risk factor history portion of the case report form is not completed, notes may appear on the case report form that refer to one or more likely risk factors. Whenever notes or comments on the case report form identify potential risk factors, LHJ surveillance staff are encouraged to conduct a follow-up investigation.

Processing ACRFs

Assigning a State ID Number - STATENO

After the HIV/AIDS Case Report Form has been completed, LHJ staff assign a new state identification number (STATENO) to each new HIV/AIDS case. This state identification number is recorded both on the paper HIV/AIDS Case Report Form and in eHARS.

In the statewide database, there is one state identification number assigned to each HIV/AIDS case. To ensure that LHJs do not use the same state identification number, the Surveillance Section allocates series of state identification numbers to each LHJ (except San Francisco and Los Angeles) and maintains a log of all assigned state identification numbers. Because reporting levels can vary between LHJs and over time, identification numbers are assigned on an as-needed basis.

Case Residency Assignment

For the purpose of HIV/AIDS reporting, the term, "case residency," means the patient's "usual residence" at the time of his or her HIV/AIDS diagnosis, regardless of where the patient is receiving care or was first infected. Case residency is the basis for allocation of local, state, and federal funds for prevention, care, and treatment services, including funds released under the Ryan White TMA.

Case residency determination requires the state, county, and Zip Codes of residence at first diagnosis. This is because geographic areas eligible to receive Ryan White Comprehensive AIDS Resource Emergency Act funds, called Eligible Metropolitan Areas (EMAs), can include a single city or a group of cities and/or counties and some EMA boundaries cross jurisdictional borders.

For reporting purposes, the patient's address is the address given by the patient at the time of HIV/AIDS diagnosis. This address, recorded in the patient's medical chart, is generally assumed to be the "usual residence."

For HIV Cases

HIV cases are assigned to a LHJ based on the date of the patient's earliest HIV diagnosis, determined by a positive confirmatory laboratory test, or when there is no laboratory test, a documented physician's diagnosis date. The HIV diagnosis date is based on the earliest, most complete date of confirmed HIV infection. In the absence of HIV laboratory test results, the date on which the patient visited the health care provider who documented the HIV diagnosis may be used as the HIV diagnosis date. When two reports of the same HIV diagnosis share the same HIV diagnosis date, case residency is determined by the date the case was entered into the surveillance system.

CDC recommends that any screening test without a positive confirmatory test be ignored for purposes of determining case residency. If the initial confirmatory results are 'indeterminate,' CDC recommends waiting for the second confirmatory result to be received before deciding to retain or delete the screening test.

For AIDS Cases

Residency at AIDS diagnosis is determined using the date the case first met the AIDS surveillance case definition. The AIDS diagnosis date is based on the earlier of: 1) the date of the first CD4+ T-lymphocyte count <200 cells/ μ L or, in the absence of the count, a CD4+ T-lymphocyte count <14 percent; or 2) the date of the patient's first diagnosed opportunistic infection. Once a case meets the AIDS surveillance definition, it never reverts to HIV.

Processing Newly Reported Cases Diagnosed in another LHJ

An HIV/AIDS case reported for an individual who resides in another LHJ or another state at the time of diagnosis is called an "out-of-jurisdiction" (OOJ) or "out-of-state" (OOS) case. HIV/AIDS case information for OOJ or OOS cases can arrive at LHJs in the form of completed HIV/AIDS Case Report Forms or laboratory test results. LHJs may also obtain HIV/AIDS case information for OOJ or OOS cases during routine active surveillance activities. The Surveillance Section is responsible for coordinating reciprocal notification and de-duplicating efforts within California and between California and other state and territorial health departments.

HIV Diagnosed in One LHJ and AIDS Diagnosed in Another

Individuals may be diagnosed with HIV in one LHJ and then progress to AIDS in another. OA considers only those cases that were first reported as HIV cases prior to the submission of an AIDS case report as eligible to become split jurisdiction cases. If an AIDS case does not have an existing HIV report at the time of the AIDS diagnosis it cannot be reported retroactively as an HIV (non-AIDS) case, regardless of the discovery of earlier clinical HIV data. In these cases individuals may have only one case report, the case report that is associated with the AIDS diagnosis.

Required Fields

In order for an LHJ's HIV/AIDS case to be considered a valid CDC-eligible case, and hence transferable to CDC, the following essential elements must be included for the case:

- STATENO
- Last Name Soundex
- Date of Birth (at least the year)
- Sex at Birth
- Vital Status or Date of Death (if deceased)

- Ethnicity/Race
- Confirmatory Lab Data or Physician Diagnosis (including date with at least the year)

XX. HIV/AIDS Case Updates, Edits, and Deletions

Once HIV/AIDS cases have been reported, it is frequently necessary to update or correct the original information. This section describes OA practices for documenting changes made to original HIV/AIDS case reports.

Editing and Updating HIV/AIDS Case Reports

It is not necessary to include all the original information on the updated form. However, at the state level, the state assigned identification number (STATENO) and the patient's name, Soundex, and birth date are necessary to identify the correct HIV/AIDS case being updated.

Case Reports Received with Incomplete or Incorrect Information

When LHJs receive an HIV/AIDS Case Report Form with missing or incorrect information, such as date of birth or name, LHJ surveillance staff must contact the health care provider to obtain the corrected information. If LHJ surveillance staff can obtain the missing information from the original reporting source before the HIV/AIDS case report has been sent to CDPH/OA's HIV/AIDS Case Surveillance Section, the updated information may be recorded on the original form.

If LHJ surveillance staff obtain the corrected information from a new data source or obtain the information after the HIV/AIDS case report has already been sent to the Surveillance Section, it is only necessary to record the corrected information on a new case report form, with a checkmark in the "update" box in the Report Status Section on the ACRF.

Case Reports with New Information

Updates are also necessary when there is new information. HIV cases that progress to AIDS would be an example of a situation where an update is needed. If an HIV/AIDS case is updated after the original HIV/AIDS Case Report Form has been sent to the Surveillance Section, the new information is documented on a separate HIV/AIDS Case Report Form. LHJ staff send the updated form to the Surveillance Section and are encouraged to keep a copy of the updated HIV/AIDS Case Report Form sent to the Surveillance Section.

HIV-to-AIDS Progression

OA considers only those cases that were first reported as HIV cases prior to the submission of an AIDS case report as eligible to become split LHJ cases. If an AIDS case does not have an existing HIV report at the time of the AIDS diagnosis, OA does not maintain this case retroactively as an HIV (non-AIDS) case, regardless of the discovery of earlier clinical HIV data. In these cases, individuals will have only one case report in eHARS, the case report that is associated with the AIDS diagnosis.

In a split LHJ case, a single individual will have one case report in eHARS for HIV infection and another case report in eHARS for AIDS. In these situations, LHJs may report the diagnosis as an AIDS case, using an HIV/AIDS Case Report Form and using the same STATENO that was used for the already reported HIV case. LHJs can obtain the STATENO from the Surveillance Section while doing case checks, and should checkmark the "update" box in the Report Status

Section on the ACRF.

XXI. Data Quality Control

Chapter Summary

The term “data quality control” as it is used here describes routine technical activities intended to identify and correct errors in collected data. Like data processing, data quality control is a critical part of ensuring the accuracy and completeness of data collected from health care providers, laboratories, and LHJs.

Errors can occur during all phases of the reporting process: data collection, data entry, and data transfer. Therefore, data quality control activities generally occur at receipt and completion of case reports; receipt of laboratory reports; and data entry. Data quality control activities also occur during data analysis. Activities described in this chapter mainly concern routine technical activities necessary for the identification and correction of common errors in electronic HIV/AIDS surveillance records. These activities include but are not limited to:

- Routine error reporting;
- Duplicate data entry; and
- Re-abstraction of records.

Outcome Standards

The following outcome standards for data accuracy and minimally allowable information are used by CDC to establish a baseline at which data is considered sufficiently reliable for analysis. These outcomes, published in *CDC/CSTE's Technical Guidance for HIV/AIDS Surveillance Programs - Data Quality*, focus on improving the quality of collected data. CDC recommends that these standards be assessed for each diagnosis year and include all cases that meet the HIV/AIDS case definitions.

Errors: At least 97 percent of case records must pass all standard data edits. Data edits identify unusual or incorrect information for one or more fields. Standard data edits are based on fields considered by CDC to be most important for data analysis (sex, date of birth, date of diagnosis, race/ethnicity, state of residence at diagnosis, initial CD4+ count at HIV and/or AIDS diagnosis, vital status, and risk factors). This assessment is to be performed for the most recent diagnosis year at 12 months after that diagnosis year.

Missing Fields: The proportion of case records missing information must be assessed for Soundex, sex, date of birth, date of diagnosis, race/ethnicity, state of residence at diagnosis, initial CD4+ count at HIV diagnosis and/or AIDS diagnosis, vital status, and date of death (for those known to be dead). The CDC-established target is 0 percent missing information.

The percentage of new cases missing information must be measured at 12 months after the diagnosis year. While a code of “unknown” is not the same as “missing,” the percentage “unknown” is also calculated. The performance standard for risk ascertainment is addressed separately.

XXII. Data Accuracy

Although data validation ensures that data entered into eHARS are reasonable and within established ranges (e.g., only numbers are entered in the Zip Code field), this activity does not check the accuracy of eHARS data.

To assist HIV/AIDS surveillance programs in prioritizing quality control activities, CDC/CSTE divide errors into two categories: major errors and minor errors. These errors are generally used in validation studies to measure the quality of reporting by health care providers as well as the quality of data collection by surveillance staff.

Major errors include:

- Any error that results in an incorrect Soundex;
- Any error in the sex, race, ethnicity, or vital status fields;
- Incorrect month or year in a date of birth, death, or diagnosis;
- Failure to obtain the earliest HIV test or first low CD4+ count;
- Omission of opportunistic illness(es);
- Omission of risk factor(s); and
- Wrong county or state in the residence at diagnosis or current residence fields.

Minor errors include:

- Omitting a suffix, such as Jr. or III in a patient's last name; and
- Incorrect or missing street address for current residence or residence at diagnosis.

Errors in Soundex and birth are of particular concern as they impact other case management activities; Soundex and birth are the two primary variables used to check for previously reported HIV/AIDS cases. In addition, many filing systems for paper HIV/AIDS case reports are based on these two fields and inaccuracies can make it difficult to locate and update these documents.

Routine Error Reporting

The Surveillance Section reviews key fields in eHARS records to identify data entry errors and missing fields that escaped notice during initial data entry. The Surveillance Section also routinely checks eHARS data for inconsistencies and duplication.

OA considers the following quality control issues when reviewing errors in collected data:

Timeliness: How long does it take to identify errors or problems in collected data and how long does it take to correct those problems? For example, inconsistencies in the data are often discovered during data analyses. If errors are consistently found during data analysis, this may indicate greater need for more frequent or complete electronic error reporting.

Error Types: Certain errors can be linked to specific parts of the reporting process. For example, inconsistencies or missing data elements may indicate a problem during data collection.

XXIII. Reporting Performance Measures

Chapter Summary

HIV/AIDS surveillance systems are routinely evaluated for accuracy, completeness, and timeliness of case reporting, and completeness and accuracy of data collected. These evaluations are used to improve eHARS, more accurately interpret analyses of data collected, and promote the best use of public health resources.

Measuring performance is an important part of promoting complete, accurate, and timely HIV/AIDS case data, and ensure a reliable source of HIV/AIDS surveillance information at the state level. Activities described in this chapter mainly concern those necessary to ensure that HIV/AIDS case reporting meets or exceeds state and national program performance standards for completeness, timeliness, duplication, risk ascertainment, and case ascertainment through death certificates.

National HIV/AIDS Performance Standards

Completeness: CDC minimum performance standard is that at least 85 percent of the expected number of HIV/AIDS cases for a diagnosis year must be reported within 12 months of the diagnosis year.

Timeliness: At least 66 percent of expected cases for a diagnosis year must be reported within 6 months of diagnosis. CDC's minimum performance standard for timeliness assessed as part of the completeness standard is 85 percent of expected HIV/AIDS case reports for a diagnosis year are reported by 12 months after the diagnosis year.

Duplication: No more than 5 percent of HIV/AIDS case reports can be duplicates or involve incorrectly matched case reports.

Risk: At least 85 percent of reported cases for a diagnosis year have an identified HIV risk factor within 12 months of the date of the initial HIV/AIDS case report, measured at 12 months after the close of the diagnosis year.

Case ascertainment through Death Certificates: The proportion of cases identified through death certificates alone should be less than 5 percent. If the proportion of such cases exceeds 5 percent, earlier reporting needs to be strengthened through other sources.

Completeness

Completeness of case reporting is estimated by dividing the observed number of HIV/AIDS cases diagnosed and reported by the expected number of HIV/AIDS diagnoses. CDC's minimum performance standard is that at least 85 percent of the expected number of HIV/AIDS cases for a diagnosis year must be reported within 12 months of the diagnosis year.

Techniques to measure completeness of reporting include capture-recapture analysis and case finding audits. This section provides a basic summary of these methods. An in-depth description of the capture-recapture technique can be found in Volume I of CDC/CSTE's Technical Guidance for HIV/AIDS Surveillance Programs Policies and Procedures (Data Quality).

The capture-recapture technique estimates the total number of expected HIV/AIDS reports for a diagnosis year based on the proportion of cases reported by two or more reporting sources. Reporting sources include but are not limited to laboratories, hospitals, health care providers, vital statistics departments, and LHJs, and the distribution of case reports by reporting source

varies between different sites. In summary, the amount of overlap of reporting from different sources is used to estimate the number of unreported HIV/AIDS diagnoses during the year. This estimate, when added to the number of reported cases, provides the total number of expected HIV/AIDS case reports.

The following criteria must be met to use the CDC capture-recapture method:

- Document-based HIV/AIDS surveillance – multiple documents from reporting sources are required to measure the overlap of reporting of individuals from different sources.
- Independent reporting sources - to avoid selection bias, reporting by one source should not impact the probability of reporting by another source.
- Equal likelihood of reporting - the probability of a case being reported by a source must be consistent over time and must be the same for all cases. Reporting sources must also cover the same geographic area.

In the absence of document-based reporting, completeness can be estimated by case finding audits, or re-abstraction studies, described earlier. Estimation of completeness requires that LHJs be able to identify all sources of reportable HIV infections and AIDS diagnoses within their jurisdictions.

Completeness for passive reporting of HIV can also be estimated through regular comparisons between reported and expected number of HIV/AIDS case reports received from an established reporting source, such as a laboratory or outpatient clinic. Using historical data to set a baseline rate, surveillance programs can monitor the volume of reporting for changes that could indicate underreporting.

Both the diagnosis facility and the report source are needed to monitor reporting trends, evaluate case ascertainment methods, and determine when active surveillance is needed. Although the report source and facility type are often the same, they describe different characteristics about the source of HIV/AIDS surveillance data.

Facility Type: The facility type describes the diagnosis setting. Analysis of HIV/AIDS cases by facility type can identify the most productive sources of surveillance case information and evaluate case ascertainment activities.

Report Source: The report source describes the method by which the case was identified and reported. When the report is initiated by the provider, the report source and facility setting will share the same code. In many circumstances, however, the report source and facility type will differ.

Measuring Timeliness

Completeness and timeliness of case reporting are interrelated measures as underreporting of cases contributes to the percentage of cases reported in a timely manner.

CDC requires that timeliness be assessed at 12 months after the diagnosis year and measured in two ways: 1) as the proportion of HIV/AIDS case reports received within 6 months of diagnosis; and 2) the proportion of expected HIV/AIDS diagnoses reported within 12 months of diagnosis.

The first timeliness measure is based on HIV/AIDS cases diagnosed and reported to the

surveillance program. Timeliness is calculated by dividing the number of HIV/AIDS cases reported within 6 months of diagnosis by the total number of reported cases for that diagnosis year. Because underreporting will overestimate timeliness, an accurate calculation of timeliness using this measure can only be made if case reporting meets the minimum standard for completeness (85 percent).

CDC's minimum performance standard for timeliness based on reported cases alone is 66 percent; at least 66 percent of expected cases for a diagnosis year must be reported within 6 months of diagnosis.

The second timeliness measure is assessed as part of the completeness standard. Timeliness for a diagnosis year is measured by dividing the number of HIV/AIDS cases reported within 12 months of diagnosis by the number of expected HIV/AIDS diagnoses.

Measuring Duplication

Duplication of HIV/AIDS case reports results in over- and under-counting, which greatly reduce the usefulness of the surveillance dataset. Duplication and incorrect matching of HIV/AIDS cases can be caused by data entry error, changes in a patient's identification information, and when patients move from one of the state's 61 LHJs to another, or out of state.

Because reportable events span the spectrum of HIV disease, it is not uncommon for an individual's case information to be reported more than once. When a patient changes health care providers, the new provider, assuming the HIV or AIDS case has not yet been reported to the state or LHJ, may submit a duplicative HIV or AIDS case report. It is not uncommon for duplicates to be identified after they have been entered into a state or national reporting system.

OA's duplicate review involves monitoring the number of duplicated and incorrectly matched cases; the proportion of these cases with exact matches on Soundex and birth date; their reporting sources (intra- versus inter-jurisdictional); and the time periods between the reports. The Surveillance Section uses this information to identify and correct problems with the collection, processing, or management of HIV/AIDS information.

CDC's standard for frequency of duplicate review in jurisdictions that have disseminated data management systems, such as California, is to conduct monthly reviews at the local level and quarterly reviews at the statewide level. In order to limit duplication in the state and national datasets, OA incorporates CDC recommended protocols into all interstate and intrastate case resolution practices and provides reciprocal notification of newly identified OOJ HIV/AIDS cases.

Duplicates Report

The Surveillance Section performs a match on eHARS records to detect potential duplicates in the HIV/AIDS surveillance data. Records are linked based on their level of agreement or disagreement on fields like name, birth date, Social Security Number, sex, and race. Linked records with incongruent dates of diagnosis or death, HIV cases known to have progressed to AIDS, twins, and other invalid duplicates are removed. Records matched on California's non-name code, linkages with weights above the set threshold value, and duplicates identified by case processors or surveillance staff are investigated further.

Routine Interstate Duplicate Review

In response to growing awareness of possible duplication of HIV and AIDS records in the

national database, CDC initiated the Routine Interstate Duplicate Review (RIDR). Through RIDR, national case reports are matched by Soundex, birth date, and gender and sent out to U.S. states and territories for resolution. California receives and subsequently resolves potential duplicate HIV/AIDS cases with other states every 6 months.

Twice a year, CDC sends California a list of RIDR cases, California HIV/AIDS cases that match by Soundex, birth date, and sex to HIV or AIDS cases reported in another U.S. state or territory. At the national level, AIDS and HIV cases are reported to CDC without personally identifying information; hence the RIDR list contains no names or Social Security Numbers. The Surveillance Section receives the RIDR list and contacts the other state or territorial HIV/AIDS surveillance coordinators to determine whether or not the linked records are true duplicates.

The Surveillance Section staff use eHARS variables, such as names, Social Security Numbers, and death and diagnosis dates to resolve potential duplicates. Potential duplicates with inconsistent death and diagnosis dates are deemed to be non-matches unless there is strong evidence that the death and diagnosis dates are incorrect.

Measuring Risk Ascertainment

Risk ascertainment is measured by dividing the number of HIV/AIDS case reports with identified HIV risk factors by the total number of reported HIV/AIDS cases. For core HIV/AIDS surveillance purposes, identified HIV risk factors include:

- Men who have sex with men (MSM);
- Injection drug users (IDU) of non-prescribed drugs received intravenously, intramuscularly, or subcutaneously;
- MSM who are also IDU;
- Heterosexual contact with a person known to have an HIV infection or a person who is at increased risk of HIV infection (e.g., an IDU who shares needles);
- Perinatal mother-to-child contact, which is when a woman who has an HIV infection, or is at increased risk of HIV infection, gives birth to a child;
- Receipt of an infusion of clotting factor blood product for treatment of hemophilia or other chronic coagulation disorder;
- Receipt of a transfusion of blood or blood components;
- Receipt of a transplant of an organ, tissue, or of artificial insemination; and
- Exposure to HIV-contaminated human body fluids by some other route (e.g., breast feeding for pediatric cases).

CDC's minimum performance standard for risk ascertainment is at least 85 percent of reported cases for a diagnosis year have an identified HIV risk factor within 12 months of the date of the initial HIV/AIDS case report, measured at 12 months after the close of the diagnosis year. This measure can be estimated based on a representative sample of reported cases.

CDC's outcome standard is appropriate for mature surveillance programs, in which the majority of new HIV/AIDS case reports is associated with incident, or newly diagnosed cases. CDC generally considers eHARS mature after 5 years of confidential, name-based reporting. This outcome standard is not suitable for case reports received during the initial 5 years of reporting. In California, AIDS became legally reportable in March 1983. California's name-based HIV reporting system was implemented in April 2006. LHJs interested in assessing the risk ascertainment outcome standard for HIV (non-AIDS) cases are encouraged to consult with the Surveillance Section for technical assistance.

LHJs may find it useful to examine the distribution of NRR cases by reporting facility on a monthly or quarterly basis. CDC's outcome standard is that 75 percent of all initial HIV/AIDS case reports have at least one HIV risk factor identified. Monitoring of cases without risk information generally involves maintaining an up-to-date NRR activity log or flagging the cases for follow up in eHARS.

Measuring Death Ascertainment Levels

Death ascertainment is measured by comparing the number of HIV/AIDS cases identified through death certificates with the number of HIV/AIDS case reports from all sources. Death certificate only (DCO) cases are those for which the death certificate is the only source of HIV/AIDS diagnosis.

Consistent with CDC guidelines for assessing this standard, the Surveillance Section calculates death ascertainment 24 months after the diagnosis year; if death information is not available within 18 months of the diagnosis year, death ascertainment is assessed 6 months after death files become available from CDPH's Office of Vital Records. The Surveillance Section matches HIV/AIDS surveillance records against statewide death records once per year. All HIV/AIDS case reports without complete death information and reports associated with individuals presumed living are included.

The Surveillance Section also measures death ascertainment by calculating the death-to-report time interval. CDC's target goal for HIV/AIDS surveillance programs is to obtain death information for cases within 24 months after the year of death. For consistency, the "report date" reflects the data entry date of the death information.

XXIV. eHARS Disaster Recovery Plan

Recovery Plan if the Network Server is Undamaged

If the OA eHARS servers are determined to be undamaged after disaster strikes, then functional recovery will require the removal of the server from the OA server room if it has sustained structural damage and is deemed an unsafe environment for service restoration. Service restoration should be initiated in the planned recovery site (OTECH) that is able to host Microsoft Windows Servers and provide an Ethernet based local area network (OSI Model) for a personal computer workstation to access the server and the eHARS database. The recovery site must also be capable of Internet access via another server so a workstation can be connected and used for the eHARS data transfer through CDC's Secure Data Network (SDN). Existing security guidelines do not allow the eHARS server to be public facing. PC workstations in the recovery site must have the required software installed (PRODAS, SAS, and Microsoft Windows XP/Win 7) to process eHARS data.

Recovery Plan if the Network Server is Damaged

If the OA eHARS servers are damaged and are unable to function adequately, then steps will be taken to acquire a new server in the planned recovery site, installation and configuration of Microsoft Windows Server with the latest Service Pack, and restoration of the files for the eHARS database from the backup tapes. If the backup tapes from the server room have also sustained damaged, then the offsite backup tapes from Iron Mountain will be used for restoring these servers. All other requirement mentioned in Item 1 also apply.

Recovery Team (eHARS Application)

Name	Role	Work Phone	Cell Phone	Home Phone
Scott Masten	Manager	(916) 449-5835	(916) 335-6872	
Curt Cadwallader	Manager	(916) 324-0820	(916) 730-1507	(916) 817-1281
Dave Rocha	Lead	(916) 449-5840	(916) 241-3647	
Ricardo Ramirez	Backup Lead	(916) 449-5837		
Fidel Encarnacion	Technical	(916) 449-5926	(916) 893-9933	(916) 685-3189

See - DRP Response Team – a full list of Stakeholders

Currently, Scott Masten, Surveillance Section Chief, owns the eHARS Application Recovery Plan. Dave Rocha is the lead for the recovery strategy. Dave Rocha and Fidel Encarnacion are the technical contacts for the recovery plan and will be responsible for the technical recovery of the eHARS application. Curt Cadwallader will be responsible for the overall management of the Recovery Team and will give orders and guidance to the team members in carrying out the recovery plan.

Dave Rocha and Ricardo Ramirez will be responsible for the eHARS application software installations. Fidel Encarnacion will be responsible for checking out the proper functionality of the server operation and connectivity if it is not physically damaged. If the server is damaged beyond operation, then he is responsible for acquiring and setting up a new server and installing the server software. Fidel will then restore the server data from the backup tapes when the server is 100% operational and fully functional.

CDPH Emergency Operations Response Plan

CDPH has outlined the department wide emergency response plan in the Emergency Operations Response Plan (EORP). This plan also includes a business continuity plan and disaster recovery plan.

XXV. Acronyms

ACRF	Adult Case Report Form
AIDS	Acquired Immunodeficiency Syndrome
C&T	Counseling and Testing
CCR	California Code of Regulations
CD	Compact Disc
CDC	Centers for Disease Control and Prevention
CDCR	California Department of Corrections and Rehabilitation
CDPH	California Department of Public Health
COPHI	Case of Public Health Importance
CSTE	Council of State and Territorial Epidemiologists
DCO	Death Certificate Only
DHAP	Divisions of HIV/AIDS Prevention
DUA	Data Use Agreement
EIA	Enzyme Immunoassay Assay
EMAs	Eligible Metropolitan Areas
HICSB	HIV Incidence and Case Surveillance Branch
HIS	HIV Incidence Surveillance
eHARS	Enhanced HIV/AIDS Reporting System
HIV	Human Immunodeficiency Virus
HSC	California Health and Safety Code
HRSA	Health Resources and Services Administration
ICD	International Classification of Diseases and Related Health Problems
ID	Identification
IT	Information Technology
LDET	Lab Data Entry Tool
LHDs	Local Health Departments
LHJs	Local Health Jurisdictions
MSM	Men who Have Sex with Men
NCHSTP	National Center for HIV, STD, and TB Prevention
NIR	No Identified Risk
NRR	No Risk Reported
OA	Office of AIDS

OIs	Opportunistic Infections
OOJ	Out-of-Jurisdiction
OOS	Out-of-State
ORP	Overall Responsible Party
PRs	Program Requirements
RIDR	Routine Interstate Duplicate Review
SFTP	Secure File Transfer Protocol
SOPs	Standard Operating Procedures
STARHS	Serologic Testing Algorithm for Recent HIV Seroconversion
STD	Sexually Transmitted Disease
TB	Tuberculosis
TMA	Ryan White HIV/AIDS Treatment Modernization Act
UID	Unique Identification
Wb	Western blot