Data Recipient Name
Agreement No. XX

CALIFORNIA ENHANCED HIV/AIDS CASE REPORTING SYSTEM
DATA USE AND DISCLOSURE AGREEMENT

This California HIV/AIDS Case Reporting System Data Use And Disclosure Agreement (hereinafter referred to as "Agreement") sets forth the information privacy and security requirements that [insert name of LHO, LHD or other recipient of data] (hereinafter "Data Recipient") is obligated to follow with respect to all HIV/AIDS Case Reporting System data, and other personal and confidential information, (as each of these types of data and information are defined herein), disclosed to Data Recipient by the California Department of Public Health (CDPH) (such Enhanced HIV/AIDS Case Reporting System [eHARS] data and other personal and confidential information are also referred to herein collectively as "Protected Data"). This Agreement covers Protected Data in any medium (paper, electronic, oral) the Protected Data exist in. By entering into this Agreement, CDPH and Data Recipient desire to protect the privacy and provide for the security of all Protected Data in compliance with all state and federal laws applicable to the Protected Data. Permission to receive and use Protected Data requires execution of this Agreement that describes the terms, conditions and limitations of Data Recipient's use of the Protected Data.

I. Supersession: This Agreement supersedes Agreement Number __None__, dated __None__, between CDPH and Data Recipient.

II. Definitions: For purposes of this Agreement, the following definitions shall apply:

A. Breach: "Breach" means:

1. The acquisition, access, use, or disclosure of Protected Data, in any medium (paper, electronic, oral), in violation of any state or federal law or in a manner not permitted under this Agreement, that compromises the privacy, security, or integrity of the information. For purposes of this definition, "compromises the privacy, security or integrity of the information" means to pose a significant risk of financial, reputational, or other harm to an individual or individuals; or

2. The same as the definition of "breach of the security of the system" set forth in California Civil Code Section 1798.29(d).

B. Confidential Information: "Confidential Information" means information that:

1. Does not meet the definition of "public records" set forth in California Government Code Section 6252, subdivision (e), or is exempt from disclosure under any of the provisions of Section 6250, et seq. of the California Government Code or any other applicable state or federal laws; or

2. Meets the definition of "confidential public health record" set forth in California Health and Safety Code Section 121035, subdivision (c); or

3. Is contained in documents, files, folders, books, or records that are clearly labeled, marked, or designated with the word "confidential" by CDPH.

Data Recipient Name
Agreement No. XX

CALIFORNIA ENHANCED HIV/AIDS CASE REPORTING SYSTEM
DATA USE AND DISCLOSURE AGREEMENT

C. Disclosure: "Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of information. "Disclosure" includes the disclosure, release, transfer, dissemination, or communication of all or any part of any confidential research record orally, in writing, or by electronic means to any person or entity, or providing the means for obtaining the records (California Health and Safety Code Sections 121035 and 121125).

D. eHARS Data: "eHARS data" means data in or from the central registry maintained by CDPH of demographic, clinical, HIV risk behavior, vital status, health facility, and administrative information on all reported HIV infections and AIDS diagnoses in California, known as eHARS. "eHARS data" specifically includes all information contained in or extracted from the following:

1. The CDPH HIV/AIDS Confidential Case Report Form, Adult (CDPH 8641A);
2. The CDPH HIV/AIDS Confidential Case Report Pediatric Form (CDPH 8641P);
3. Birth certificate document;
4. Death document;
5. Laboratory document;
6. Pre-test document;
7. Post-test document; or
8. Administrative data (document identification, system dates) from eHARS.

E. Personal Information: "Personal Information" means information that:

1. By itself, directly identifies, or uniquely describes an individual; or
2. Creates a substantial risk that it could be used in combination with other information to indirectly identify or uniquely describe an individual, or link an individual to the other information; or
3. Meets the definition of "personal information" set forth in California Civil Code section 1798.3, subdivision (a); or
4. Is one of the data elements set forth in California Civil Code section 1798.29, subdivisions (e)(1), (2) or (3); or
5. Meets the definition of "medical information" set forth in either California Civil Code section 1798.29, subdivision (f)(2) or California Civil Code section 56.05, subdivision (g); or

6. Meets the definition of "health insurance information" set forth in California Civil Code section 1798.29, subdivision (f)(3).

F. Protected Data: "Protected Data" means data that consists of one or more of the following types of information:

1. "eHARS Data", as defined above; or

2. "Confidential Information", as defined above.

3. "Personal Information", as defined above; or

G. Security Incident: "Security Incident" means:

1. An attempted breach; or

2. The attempted or successful modification or destruction of Protected Data, in violation of any state or federal law or in a manner not permitted under this Agreement; or

3. The attempted or successful modification or destruction of, or interference with, Data Recipient's system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of Protected Data, or hinders or makes impossible Data Recipient's receipt, collection, creation, storage, transmission or use of Protected Data by Data Recipient pursuant to this Agreement.

H. Use: "Use" means the sharing, employment, application, utilization, examination, or analysis of information.

III. Background and Purpose: The CDPH, Office of AIDS (OA) is designated by the California Health and Safety Code Section 131019 as the lead agency for coordinating state programs, services, and activities relating to HIV/AIDS. The primary mission of OA is to assess, prevent, and interrupt the transmission of HIV and to provide for the needs of infected Californians by identifying the scope and extent of HIV infection, providing for the needs which it creates, and disseminating timely and complete information. OA is responsible for oversight of HIV/AIDS case reporting in California and as such, maintains eHARS, a confidential, central registry of demographic and clinical information on all reported HIV infections and AIDS diagnoses in California. Case counts generated by this reporting system are used to inform funding allocations for such programs and activities as the Ryan White Program, Federal Centers for Disease Control and Prevention (CDC) prevention, and surveillance. The Health Resources and Services Administration uses HIV and AIDS case counts to determine Ryan White funding levels. Through Ryan White, 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. eHARS collects data to support HIV/AIDS surveillance according to CDC standards. Thus, the system is designed

to collect, organize, manage, store, and retrieve data CDC has identified as necessary to conduct HIV/AIDS case surveillance statewide.

The purpose of this Agreement is to permit exchange of eHARS information between California's local health jurisdictions and CDPH. This exchange is necessitated by California Code of Regulations (Title 17, Sections 2502, 2505, and 2641.5 through 2643.20), which dictates that case report information from laboratories and health care providers is reportable to the local health officer who thereafter reports this information to CDPH (a decentralized system). California's decentralized eHARS thus facilitates local as well as CDPH access to eHARS data to facilitate local care, prevention, and surveillance activity, including local application to Federal Ryan White Part A funds and locally tailored prevention services.

IV. Legal Authority for Disclosure and Use of Protected Data: The legal authority for CDPH to collect, use, and disclose Protected Data, and for Data Recipient to receive and use Protected Data is as follows:

A. General Legal Authority:

List of Reportable Diseases and Conditions:

1. California Health and Safety Code Section 120130 provides in part as follows: "The department shall establish a list of reportable diseases and conditions. For each reportable disease and condition, the department shall specify the timeliness of requirements related to the reporting of each disease and condition, and the mechanisms required for, and the content to be included in, reports made pursuant to this section. The list of reportable diseases and conditions may include both communicable and noncommunicable diseases. Those diseases listed as reportable shall be properly reported as required to the department by the health officer . . . ."

2. Title 17, California Code of Regulations, Section 2500, subdivision (g), provides in part as follows: "Upon the State Department of Public Health's request, a local health department shall provide to the department the information reported pursuant to this section . . . ."

B. California HIV/AIDS-Specific Legal Authority:

1. Disclosure Permitted for Public Health Purposes: California Health and Safety Code Section 121025, subdivision (a) provides as follows: "Public health records relating to [HIV/AIDS], containing personally identifying information, that were developed or acquired by state or local public health agencies, or an agent of such an agency, shall be confidential and shall not be disclosed, except as otherwise provided by law for public health purposes . . . ."

2. Disclosure Permitted to Carry Out the Investigation, Control, or Surveillance Duties of CDPH and Data Recipient: California Health and Safety Code Section 121025, subdivision (b), provides as follows: "In accordance with subdivision (g) of Section 121022, a state or local

public health agency, or an agent of such an agency, may disclose personally identifying information in public health records . . . to other local, state, or federal public health agencies . . . when the confidential information is necessary to carry out the duties of the agency . . . in the investigation, control, or surveillance of disease, as determined by the state or local public health agency."

3. Further Disclosure Permitted For Public Health Purposes: California Health and Safety Code Section 121025, subdivision (c) provides as follows: "Except as provided in paragraphs (1) to (3), inclusive, any disclosure authorized by subdivision (a) or (b) shall include only the information necessary for the purpose of that disclosure and shall be made only upon agreement that the information will be kept confidential and will not be further disclosed without written authorization, as described in subdivision (a). . . ."

4. Only Minimum Necessary Disclosure Permitted: California Health and Safety Code Section 121025, subdivision (c), provides as follows: "Any disclosure authorized . . . shall include only the information necessary for the purpose of that disclosure . . . ."

5. Agreement Required: California Health and Safety Code Section 121025, subdivision (c), provides as follows: "[Disclosure] shall be made only upon agreement that the information will be kept confidential and will not be further disclosed without written authorization [by the subject of the information] . . . ."

6. No Liability for HIV/AIDS Reporting: California Health and Safety Code Section 120980, subdivision (i), provides an exemption from liability for disclosure of HIV/AIDS reporting: "Nothing in this section imposes liability or criminal sanction for disclosure of an HIV test, as defined in subdivision (c) of Section 120775, in accordance with any reporting requirement for a case of HIV infection, including AIDS by the [California Department of Public Health] . . . ."

7. AIDS Reporting: Title 17, California Code of Regulations, Section 2502, subdivision (b), provides in part as follows: Individual Case and Outbreak Reports: For the diseases listed below, the local health officer shall prepare and send to the Department along with the summary report described in (a) above an individual case or outbreak report for each individual case/outbreak of those diseases which the Department has identified as requiring epidemiological analysis reported pursuant to Section 2500. At the discretion of the director, the required individual case/outbreak report may be either a Confidential Morbidity Report (PM-110 1/90), its electronic equivalent or a hard copy 8.5 x 11 inch individual case/outbreak report form. The Weekly Morbidity by Place of Report form (DHS 8245 11/95) indicates which format to use. Each individual case report shall include the following: 1) verification of information reported pursuant to Section 2500; 2) information on the probable source of infection, if known; 3) laboratory or radiologic findings, if any; 4) clinical signs and/or symptoms, if applicable; and 5) any known epidemiological risk factors . . . "An individual case report is required for the following diseases: Acquired Immune Deficiency Syndrome (AIDS). . ."

CALIFORNIA ENHANCED HIV/AIDS CASE REPORTING SYSTEM
DATA USE AND DISCLOSURE AGREEMENT

8. HIV Infection Reporting:

   a. California Health and Safety Code Section 121022, subdivision (a) provides: "To ensure knowledge of current trends in the HIV epidemic and to assure that California remains competitive for federal HIV and AIDS funding, health care providers and laboratories shall report cases of HIV infection to the local health officer using patient names. Local health officers shall report unduplicated HIV cases by name to the [California Department of Public Health]."

   b. California Health and Safety Code Section 121022, subdivision (f) provides: "State and local health department employees and contractors shall be required to sign confidentiality agreements developed by the department that include information related to the penalties for a breach of confidentiality, and the procedures for reporting a breach of confidentiality . . ."

   c. California Health and Safety Code Section 121023, subdivision (a) provides: "Subject to subdivision (b), each clinical laboratory, as defined in Section 1206 of the Business and Professions Code, shall report all CD4+ T-Cell Test results to the local health officer for the local health jurisdiction where the health care provider facility is located within seven days of the completion of the CD4+ T-Cell test. . . ."

   d. Title 17, California Code of Regulations, Section 2643.15, provides in part as follows: "The local health officer or his or her authorized designee shall match and induplicate laboratory reports of confirmed HIV tests with the local health department HIV/AIDS registry database and with HIV/AIDS case reports received from health care providers and not entered into the database. The health officer or his or her authorized designee shall, within 45 calendar days of receipt of a laboratory report of a confirmed HIV test, submit unduplicated HIV/AIDS case reports to the Department."

C. Health Insurance Portability and Accountability Act (HIPAA) Authority:

1. CDPH HIPAA Status: CDPH is a "hybrid entity" for purposes of applicability of the federal regulations entitled, "Standards for Privacy of Individually Identifiable Health Information," ("Privacy Rule") (Title 45, Code of Federal Regulations, Parts 160, 162, and 164) promulgated pursuant to HIPAA (Title 42, United States Code, Sections 1320d - 1320d-8). All of the CDPH programs that collect, use, or disclose Protected Data have been designated by CDPH as HIPAA-covered "health care components" of CDPH. (Title 45, Code of Federal Regulations, Section 164.504(c)(3)(iii).)

2. Parties Are "Public Health Authorities": CDPH and Data Recipient are each a "public health authority" as that term is defined in the Privacy Rule. (Title 45, Code of Federal Regulations, Sections 164.501 and 164.512(b)(1)(i).)

CALIFORNIA ENHANCED HIV/AIDS CASE REPORTING SYSTEM
DATA USE AND DISCLOSURE AGREEMENT

3. Protected Data Use and Disclosure Permitted by HIPAA: To the extent a disclosure or use of Protected Data is a disclosure or use of "Protected Health Information" (PHI) of an individual, as that term is defined in Section 160.103 of Title 45, Code of Federal Regulations, the following Privacy Rule provisions apply to permit such Protected Data disclosure and/or use by CDPH and Data Recipient, without the consent or authorization of the individual who is the subject of the PHI:

   a. The HIPAA Privacy Rule creates a special rule for a subset of public health disclosures whereby HIPAA cannot preempt state law if, "[t]he provision of state law, including state procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention." (Title 45, Code of Federal Regulations, Section 160.203(c).) [NOTE: See Sections IV.A and IV.B, above.];

   b. A covered entity may disclose PHI to a "public health authority" carrying out public health activities authorized by law; (Title 45, Code of Federal Regulations, Section 164.512(b).); and

   c. Other, non-public health-specific provisions of HIPAA may also provide the legal basis for all or specific Protected Data uses and disclosures.

V. Disclosure Restrictions: The Data Recipient, and its employees or agents, shall protect from unauthorized disclosure any Protected Data. The Data Recipient shall not disclose, except as otherwise specifically permitted by this Agreement, any Protected Data to anyone other than CDPH, except if disclosure is allowed or required by state or federal law.

VI. Use Restrictions: The Data Recipient, and its employees or agents, shall not use any Protected Data for any purpose other than carrying out the Data Recipient's obligations under the statutes and regulations set forth in Section IV, above, or as otherwise allowed or required by state or federal law.

VII. Safeguards: Data Recipient shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of Protected Data, including electronic or computerized Protected Data. The Data Recipient shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Data Recipient's operations and the nature and scope of its activities in performing its legal obligations and duties (including performance of its duties and obligations under this Agreement), and which incorporates the requirements of Section VIII, Security, below. Data Recipient shall provide CDPH with Data Recipient's current and updated policies.

VIII. Security: The Data Recipient shall take all steps necessary to ensure the continuous security of all computerized data systems containing Protected Data. These steps shall include, at a minimum:

CALIFORNIA ENHANCED HIV/AIDS CASE REPORTING SYSTEM
DATA USE AND DISCLOSURE AGREEMENT

A. Complying with all of the data system security precautions listed in the Data Recipient Data Security Standards set forth in Attachment A to this Agreement;

B. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

In case of a conflict between any of the security standards contained in any of the aforementioned sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to Protected Data from breaches and security incidents.

IX. Security Officer: The Data Recipient shall designate a Security Officer to oversee its compliance with this Agreement and for communicating with CDPH on matters concerning this Agreement.

X. Training: The Data Recipient shall provide training on its obligations under this Agreement, at its own expense, to all of its employees who assist in the performance of Data Recipient's obligations under this Agreement, or otherwise use or disclose Protected Data.

A. The Data Recipient shall require each employee who receives training to sign a certification, indicating the employee's name and the date on which the training was completed.

B. The Data Recipient shall retain each employee's written certifications for CDPH inspection for a period of three years following contract termination.

XI. Employee Discipline: Data Recipient shall discipline such employees and other Data Recipient workforce members who intentionally violate any provisions of this Agreement, including, if warranted, by termination of employment.

XII. Employee/Contractor Security and Confidentiality Agreement: Prior to accessing protected data, Data Recipient employees and contractors will sign CDPH's confidentiality agreement, provide signed copies of these agreements to CDPH and review these agreements annually as required by law (See Attachment B, "Agreement by Employee/Contractor to Comply with Confidentiality Requirements" (CDPH 8689)).

XIII. Breach and Security Incident Responsibilities:

A. Notification to CDPH of Breach or Security Incident: The Data Recipient shall notify CDPH **immediately by telephone call plus e-mail or fax** upon the discovery of a breach (as defined in this Agreement), **or** within **24 hours by e-mail or fax** of the discovery of any security incident (as defined in this Agreement). Notification shall be provided to the CDPH Program Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer, using the contact

information listed in Section XII (E), below. If the breach or security incident occurs after business hours or on a weekend or holiday and involves Protected Data in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH Information Technology Service Desk at the telephone numbers listed in Section XII (E), below. For purposes of this section, breaches and security incidents shall be treated as discovered by Data Recipient as of the first day on which such breach or security incident is known to the Data Recipient, or, by exercising reasonable diligence would have been known to the Data Recipient. Data Recipient shall be deemed to have knowledge of a breach or security incident if such breach or security incident is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach or security incident, who is an employee or agent of the Data Recipient.

Data Recipient shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment; and

2. Any action pertaining to a breach required by applicable federal and state laws, including, specifically, California Civil Code Section 1798.29.

B. Investigation of Breach: The Data Recipient shall immediately investigate such breach or security incident, and within 72 hours of the discovery, shall inform the CDPH Program Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer of:

1. What data elements were involved and the extent of the data involved in the breach, including, specifically, the number of individuals whose personal information was breached; and

2. A description of the unauthorized persons known or reasonably believed to have improperly used the Protected Data and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the Protected Data, or to whom it is known or reasonably believed to have had the Protected Data improperly disclosed to them; and

3. A description of where the Protected Data is believed to have been improperly used or disclosed; and

4. A description of the probable causes of the breach or security incident; and

5. Whether California Civil Code Section 1798.29 or any other federal or state laws requiring individual notifications of breaches have been triggered.

C. Written Report: The Data Recipient shall provide a written report of the investigation to the CDPH Program Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer within five working days of the discovery of the breach or security incident. The report shall

include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the breach or security incident, and measures to be taken to prevent the recurrence of such breach or security incident.

D. Notification to Individuals: If notification to individuals whose information was breached is required under state or federal law, and regardless of whether Data Recipient is considered only a custodian and/or non-owner of the Protected Data, Data Recipient shall, at its sole expense, and at the sole election of CDPH, either:

1. Make notification to the individuals affected by the breach (including substitute notification), pursuant to the content and timeliness provisions of such applicable state or federal breach notice of laws. The CDPH Privacy Officer shall approve the time, manner and content of any such notifications, prior to the transmission of such notifications to the individuals; or

2. Cooperate with and assist CDPH in its notification (including substitute notification) to the individuals affected by the breach.

E. CDPH Contact Information: To direct communications to the above referenced CDPH staff, the Data Recipient shall initiate contact as indicated herein. CDPH reserves the right to make changes to the contact information below by giving written notice to the Data Recipient. Said changes shall not require an amendment to this Agreement.

CDPH Program Manager	**CDPH Privacy Officer**	**CDPH Chief Information Security Officer (and CDPH IT Service Desk)**
Deanna Sykes, Surveillance, Section Chief Office of AIDS, CDPH, MS 7700, P.O. Box 997426 Sacramento, CA 95899-7426 Deanna.Sykes@cdph.ca.gov Telephone: (916) 449-5835 Fax: (916) 449-5861	Privacy Officer Privacy Office, Office of Legal Services, CDPH 1415 L Street, Suite 600 Sacramento, CA 95814 privacy@cdph.ca.gov Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office, CDPH, MS 6302 P.O. Box 997377 Sacramento, CA 95899-7377 cdphiso@cdph.ca.gov Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

XIV. Indemnification: Data Recipient shall indemnify, hold harmless and defend CDPH from and against any and all claims, losses, liabilities, damages, costs and other expenses (including attorney's fees) that result from or arise directly or indirectly out of or in connection with any negligent act or omission or willful misconduct of Data Recipient, its officers, employees or agents relative to the Protected Data, including without limitation, any violations of Data Recipient's responsibilities under this Agreement.

CALIFORNIA ENHANCED HIV/AIDS CASE REPORTING SYSTEM
DATA USE AND DISCLOSURE AGREEMENT

XV. Term of Agreement: This Agreement shall remain in effect for five years after the latest signature date in the signature block below. After five years, this Agreement will expire without further action. If the parties wish to extend this Agreement, they may do so by reviewing, updating, and reauthorizing this Agreement. The newly signed agreement should explicitly supersede this Agreement, which should be referenced by Agreement Number and date in Section I of the new Agreement. If one or both of the parties wish to terminate this Agreement prematurely, they may do so upon 30 days advanced notice. CDPH may also terminate this Agreement pursuant to Section XV or XVII, below.

XVI. Termination for Cause:

A. Termination Upon Breach: A breach by Data Recipient of any provision of this Agreement, as determined by CDPH, shall constitute a material breach of the Agreement and grounds for immediate termination of the Agreement by CDPH. At its sole discretion, CDPH may give Data Recipient 30 days to cure the breach.

B. Judicial or Administrative Proceedings: Data Recipient will notify CDPH if it is named as a defendant in a criminal proceeding related to a violation of this Agreement. CDPH may terminate the Agreement if Data Recipient is found guilty of a criminal violation related to a violation of this Agreement. CDPH may terminate the Agreement if a finding or stipulation that the Data Recipient has violated any security or privacy laws is made in any administrative or civil proceeding in which the Data Recipient is a party or has been joined.

XVII. Return or Destruction of Protected Data on Expiration or Termination: On expiration or termination of the agreement between Data Recipient and CDPH for any reason, Data Recipient shall return or destroy the Protected Data. If return or destruction is not feasible, Data Recipient shall explain to CDPH why, in writing, to the CDPH Program Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer, using the contact information listed in Section XIII (E), above.

A. Retention Required by Law: If required by state or federal law, Data Recipient may retain, after expiration or termination, Protected Data for the time specified as necessary to comply with the law.

B. Obligations Continue Until Return or Destruction: Data Recipient's obligations under this Agreement shall continue until Data Recipient destroys the Protected Data or returns the Protected Data to CDPH; provided however, that on expiration or termination of the Agreement, Data Recipient shall not further use or disclose the Protected Data except as required by state or federal law.

C. Notification of Election to Destroy Protected Data: If Data Recipient elects to destroy the Protected Data, Data Recipient shall certify in writing, to the CDPH Program Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer, using the contact information listed in Section XIII (E), above, that the Protected Data has been destroyed.

Data Recipient Name
Agreement No. XX

CALIFORNIA ENHANCED HIV/AIDS CASE REPORTING SYSTEM
DATA USE AND DISCLOSURE AGREEMENT

XVIII. Amendment: The parties acknowledge that federal and state laws relating to information security and privacy are rapidly evolving and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of Protected Data. Upon CDPH request, Data Recipient agrees to promptly enter into negotiations with CDPH concerning an amendment to this Agreement embodying written assurances consistent with new standards and requirements imposed by regulations and other applicable laws. CDPH may terminate this Agreement upon 30-days written notice in the event:

A. Data Recipient does not promptly enter into negotiations to amend this Agreement when requested by CDPH pursuant to this section; or

B. Data Recipient does not enter into an amendment providing assurances regarding the safeguarding of Protected Data that CDPH in its sole discretion deems sufficient to satisfy the standards and requirements of applicable laws and regulations relating to the security or privacy of Protected Data.

XIX. Assistance in Litigation or Administrative Proceedings: Data Recipient shall make itself and any employees or agents assisting Data Recipient in the performance of its obligations under this Agreement, available to CDPH at no cost to CDPH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CDPH, its director, officers or employees based upon claimed violation of laws relating to security and privacy, which involves inactions or actions by the Data Recipient, except where Data Recipient or its employee or agent is a named adverse party.

XX. Disclaimer: CDPH makes no warranty or representation that compliance by Data Recipient with this Agreement will be adequate or satisfactory for Data Recipient's own purposes or that any information in Data Recipient's possession or control, or transmitted or received by Data Recipient, is or will be secure from unauthorized use or disclosure. Data Recipient is solely responsible for all decisions made by Data Recipient regarding the safeguarding of Protected Data.

XXI. Transfer of Rights: Data Recipient has no right and shall not subcontract, delegate, assign, or otherwise transfer or delegate any of its rights or obligations under this Agreement to any other person or entity. Any such transfer of rights shall be null and void.

XXII. No Third-Party Beneficiaries: Nothing expressed or implied in the terms and conditions of this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Data Recipient and their respective successors or assignees, any rights, remedies, obligations or liabilities, whatsoever.

XXIII. Interpretation: The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with regulations and applicable State and Federal laws. The

parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that complies and is consistent with federal and state laws.

XXIV. Survival: The respective rights and obligations of Data Recipient under Sections VII, VIII and XII of this Agreement shall survive the termination or expiration of this Agreement .

XXV. Entire Agreement: This Agreement constitutes the entire agreement between CDPH and Data Recipient. Any and all modifications of this Agreement must be in writing and signed by all parties. Any oral representations or agreements between the parties shall be of no force or effect.

XXVI. Severability: The invalidity in whole or in part of any provisions of this Agreement shall not void or affect the validity of any other provisions of this Agreement.

XXVII. Signatures:

IN WITNESS, WHEREOF, the Parties have executed this Agreement as follows:

On behalf of the Data Recipient, [insert name of LHO, LHD or other recipient of data] , the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to abide by and enforce all the terms specified herein.

_____
(Name of Representative of [insert name of LHO, LHD or other recipient of data]

_____ (Title)

_____
(Signature) (Date)

On behalf of CDPH, the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

_____
(Name of CDPH Representative)

_____
(Title)

_____

(Signature) (Date)

Data Recipient Name
Agreement No. XX

CALIFORNIA ENHANCED HIV/AIDS CASE REPORTING SYSTEM
DATA USE AND DISCLOSURE AGREEMENT

Attachment A

Data Recipient Data Security Standards

1. General Security Controls

a. ***Confidentiality Statement.*** All persons that will be working with Protected Data must sign a confidentiality statement. The statement must include at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to Protected Data. The statement must be renewed annually. The Data Recipient shall retain each person's written confidentiality statement for CDPH inspection for a period of three years following contract termination.

b. ***Background check.*** Before a member of the Data Recipient's workforce may access Protected Data, Data Recipient must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk for theft of confidential data. The Data Recipient shall retain each workforce member's background check documentation for a period of three years following contract termination.

c. ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store Protected Data must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. The encryption solution must be full disk unless approved by the CDPH Information Security Office.

d. ***Server Security.*** Servers containing unencrypted Protected Data must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

e. ***Minimum Necessary.*** Only the minimum necessary amount of Protected Data required to perform necessary business functions may be copied, downloaded, or exported.

f. ***Removable media devices.*** All electronic files that contain Protected Data 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.). Must be encrypted using a FIPS 140-2 certified algorithm, such as AES, with a 128bit key or higher.

g. ***Antivirus software.*** All workstations, laptops, and other systems that process and/or store Protected Data must install and actively use a comprehensive anti-virus software solution with automatic updates scheduled at least daily.

h. ***Patch Management.*** All workstations, laptops, and other systems that process and/or store Protected Data must have security patches applied, with system reboot if necessary. There must be a documented patch management process which determines

installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

i. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing Protected Data. Username must be promptly disabled, deleted, or the

password changed upon the transfer or termination of an employee with knowledge of the password. Passwords: are not to be shared; must be at least eight characters; must be a non-dictionary word; must not be stored in readable format on the computer; must be changed every 60 days; must be changed if revealed or compromised and must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z);
- Lower case letters (a-z);
- Arabic numerals (0-9); and
- Non-alphanumeric characters (punctuation symbols).

j. ***Data Sanitization.*** All Protected Data must be sanitized using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.

2. System Security Controls

a. ***System Timeout.*** The system must provide an automatic timeout, requiring reauthentication of the user session after no more than 20 minutes of inactivity.

b. ***Warning Banners.*** All systems containing Protected Data must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.

c. ***System Logging.*** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for Protected Data, or which alters Protected Data. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If Protected Data is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three years after occurrence.

d. ***Access Controls.*** The system must use role based access controls for all user authentications, enforcing the principle of least privilege.

e. ***Transmission encryption.*** All data transmissions of Protected Data outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as AES, with a 128bit key or higher. Encryption can be end to end at the network level, or the

data files containing Protected Data can be encrypted. This requirement pertains to any type of Protected Data in motion such as website access, file transfer, and e-mail.

f. ***Intrusion Detection***. All systems involved in accessing, holding, transporting, and protecting Protected Data that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

a. ***System Security Review.*** All systems processing and/or storing Protected Data must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.

b. ***Log Reviews.*** All systems processing and/or storing Protected Data must have a routine procedure in place to review system logs for unauthorized access.

c. ***Change Control.*** All systems processing and/or storing Protected Data must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. Business Continuity/Disaster Recovery Controls

a. ***Disaster Recovery.*** Data Recipient must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic Protected Data in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this agreement for more than 24 hours.

b. ***Data Backup Plan.*** Data Recipient must have established documented procedures to back-up Protected Data to maintain retrievable exact copies of Protected Data. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of back-up media, and the amount of time to restore Protected Data should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDPH data.

5. Paper Document Controls

a. ***Supervision of Data.*** Protected Data in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Protected Data in paper form shall not be left unattended at any time in vehicles, planes, trains, or any other modes of transportation and shall not be checked in baggage on commercial airplanes.

CALIFORNIA ENHANCED HIV/AIDS CASE REPORTING SYSTEM
DATA USE AND DISCLOSURE AGREEMENT

b. ***Escorting Visitors.*** Visitors to areas where Protected Data is contained shall be escorted and CDPH PHI shall be kept out of sight while visitors are in the area.

c. ***Confidential Destruction.*** Protected Data must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.

d. ***Removal of Data.*** Protected Data must not be removed from the premises of the Data Recipient except with express written permission of CDPH.

e. ***Faxing.*** Faxes containing Protected Data shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending.

f. ***Mailing.*** Protected Data shall only be mailed using secure methods. Large volume mailings of CDPH PHI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a CDPH-approved solution, such as a solution using a vendor product specified on the CSSI.

Data Recipient Name
Agreement No. XX

CALIFORNIA ENHANCED HIV/AIDS CASE REPORTING SYSTEM DATA USE AND DISCLOSURE AGREEMENT

Attachment B

State of California—Health and Human Services Agency California Department of Public Health
Office of AIDS

Agreement by Employee/Contractor to Comply with Confidentiality Requirements

Summary of Statutes Pertaining to Confidential Public Health Records and Penalties for Disclosure

All HIV/AIDS case reports and any information collected or maintained in the course of surveillance-related activities that may directly or indirectly identify an individual are considered *confidential public health record(s)* under California Health and Safety Code (HSC), Section 121035(c) and must be handled with the utmost confidentiality. Furthermore, HSC §121025(a) prohibits the disclosure of HIV/AIDS-related public health records that contain any personally identifying information to any third party, unless authorized by law for public health purposes, or by the written consent of the individual identified in the record or his/her guardian/conservator. 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 §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-$25,000 plus court costs as provided by HSC §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 $25,000 plus court costs (HSC §121025(e)(3)). Any person who is guilty of a confidentiality infringement of the foregoing type 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 §121025(e)(4)). Each disclosure in violation of California law is a separate, actionable offense (HSC §121025(e)(5)).

Because an assurance of case confidentiality is the foremost concern of the California Department of Public Health, Office of AIDS (CDPH/OA), any actual or potential breach of confidentiality shall be immediately reported. In the event of any suspected breach, staff shall immediately notify the director or supervisor of the local health department's HIV/AIDS surveillance unit who in turn shall notify the CDPH/OA Surveillance Section Chief or designee. CDPH/OA, in conjunction with the local health department and the local health officer shall promptly investigate the suspected breach. Any evidence of an actual breach shall be reported to the law enforcement agency that has jurisdiction.

Employee Confidentiality Pledge

I recognize that in carrying out my assigned duties, I may obtain access to private information about persons diagnosed with HIV or AIDS that was provided under an assurance of confidentiality. I understand that I am prohibited from disclosing or otherwise releasing any personally identifying information, either directly or indirectly, about any individual named in any HIV/AIDS confidential public health record. Should I be responsible for any breach of confidentiality, I understand that civil and/or criminal penalties may be brought against me. I acknowledge that my responsibility to ensure the privacy of protected health information contained in any electronic records, paper documents, or verbal communications to which I may gain access shall not expire, even after my employment or affiliation with the Department has terminated.

By my signature, I acknowledge that I have read, understand, and agree to comply with the terms and conditions above.

_____	_____	_____
Employee name (print)	Employee Signature	Date
_____	_____	_____
Supervisor name (print)	Supervisor Signature	Date

_____
Name of Employer

PLEASE RETAIN A COPY OF THIS DOCUMENT FOR YOUR RECORDS.

CDPH 8 6 8 9 (Revised 10/12)