CalREDIE System Data Use And Disclosure Agreement

This California Reportable Disease Information Exchange (**CalREDIE**) System Data Use And Disclosure Agreement ("Agreement") sets forth the information privacy and security requirements that the San Bernardino County **Department of Public Health** ("Participant"), and the California Department of Public Health ("CDPH") are obligated to follow with respect to all CalREDIE Data (as defined herein) collected or created within the CalREDIE System. By entering into this Agreement, CDPH and Participant agree to protect the privacy and provide for the security of all CalREDIE Data in compliance with all state and federal laws applicable to the CalREDIE Data. Permission to receive, use and disclose CalREDIE Data requires execution of this Agreement that describes the terms, conditions, and limitations of Participant's collection, use, and disclosure of the CalREDIE Data.

I. Supersession: This Agreement supersedes any prior CalREDIE Agreement between CDPH and Participant.

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

A. Breach: "Breach" means:

1. the acquisition, access, use, or disclosure of CalREDIE Data 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 poses 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, subdivision (f). The "system" referenced in Civil Code section 1798.29 shall be interpreted for purposes of this Agreement to reference the California Reportable Disease Information Exchange (CalREDIE) System, only.

B. California Reportable Disease Information Exchange (CalREDIE) System Data: "California Reportable Disease Information Exchange (CalREDIE) System Data" means data in the state-wide reportable disease database supported and maintained by CDPH including demographic, epidemiologic (including clinical information, risk factor information, and laboratory test result information), and administrative information on reportable diseases collected for the purposes of case investigation, disease prevention, and surveillance.

1. CalREDIE Data specifically includes information contained in or derived from the following:

a. Confidential Morbidity Report (CMR) required by Title 17 of the California Code of Regulations (CCR) sections 2500, 2593, 2641.5-2643.20, and 2800-2812 Reportable Diseases and Conditions.

b. Laboratory Test and Result information required by Title 17 of the CCR sections 2505 and 2641.5 - 2643.20.

c. Communicable Disease Control Report Forms (required for specific diseases and conditions that are mandated by state laws and regulations to be reported by healthcare providers and laboratories to local health officers).

2. CalREDIE Data specifically excludes the following information:

a. [Reserved.]

C. Disclosure: "Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of information.

D. Security Incident: "Security Incident" means:

1. an attempted breach;

2. the attempted or successful modification or destruction of CalREDIE Data in the California Reportable Disease Information Exchange (CalREDIE) System, 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, system operations in the California Reportable Disease Information Exchange (CalREDIE) System that negatively impacts the confidentiality, availability or integrity of CalREDIE Data, or hinders or makes impossible the receipt, collection, creation, storage, transmission or use of CalREDIE Data in the CalREDIE System.

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

F. Workforce Member: "Workforce Member" means an employee, volunteer, trainee, or other person whose conduct, in the performance of work for Participant, is under the direct control of Participant, whether or not they are paid by the Participant.

G. [Reserved.]

III. Background and Purpose: The California Reportable Disease Information Exchange (CalREDIE) System is a system of applications that encompasses the core surveillance and reporting application, electronic laboratory reporting (ELR) application, ELR message handling application, provider reporting application, alerting and notification application, Data Warehouse (DW), and Data Distribution Portal (DDP) that the CDPH has implemented for web-based disease reporting and surveillance. The purpose of this application is to improve the efficiency of surveillance activities and the early detection of public health events through the collection of more complete and timely surveillance information on a statewide basis. CalREDIE is a secure, web-based electronic solution

for health care providers to report cases of conditions of public health interest; and for laboratories to report laboratory reports for notifiable conditions to LHDs and the CDPH, and for LHDs to report conditions to CDPH. CalREDIE is an integral part of the overall California public health emergency preparedness and response strategy where completion and implementation of CalREDIE allows for 24/7/365 reporting and receipt of notifiable conditions. LHDs and CDPH have access to disease and laboratory reports in near real-time for disease surveillance, public health investigation, and case management activities. CalREDIE is the system of record for communicable disease surveillance data within California.

IV. Legal Authority for Collection, Use and Disclosure of CalREDIE Data: The legal authority for CDPH and Participant to collect, use and disclose CalREDIE Data is set forth in Attachment A, which is made part of this Agreement by this reference.

V. Health Insurance Portability and Accountability Act of 1996 (HIPAA) Authority:

A. CDPH and CalREDIE 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") (45 C.F.R. Parts 160, 162, and 164) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. §§ 1320d - 1320d-8) (as amended by Subtitle D Privacy, of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111–5, 123 Stat. 265–66)). The CalREDIE System has not been designated by the CDPH as, and is not, one of the HIPAA-covered "health care components" of CDPH. (45 C.F.R. §164.103.) The legal basis for this determination is as follows:

1. The CalREDIE System is not a component of CDPH that would meet the definition of a covered entity or business associate if it were a separate legal entity. (45 C.F.R. §§164.105(a)(2)(iii)(D); 160.103 (definition of "covered entity").) And

2. The HIPAA Privacy Rule creates a special rule for a subset of public health activities 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." (45 C.F.R. § 160.203(c) [HITECH Act, § 13421, sub. (a)].) [NOTE: See state laws and regulations listed in Attachment A.]

B. Parties Are "Public Health Authorities": CDPH and Participant are each a "public health authority" as that term is defined in the Privacy Rule. (45 C.F.R. §§ 164.501; 164.512(b)(1)(i).)

C. CalREDIE Data Use and Disclosure Permitted by HIPAA: To the extent a disclosure or use of CalREDIE Data may also be considered 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 CalREDIE Data disclosure and/or use by CDPH and Participant, without the consent or authorization of the individual who is the subject of the PHI:

1. 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." (45 C.F.R. § 160.203(c) [HITECH Act, § 13421, sub. (a)].) [NOTE: See state laws and regulations listed in Attachment A];

2. A covered entity may disclose PHI to a "public health authority" carrying out public health activities authorized by law; (45 C.F.R. § 164.512(b).);

3. A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law." (45 C.F.R. §§ 164.502 (a)(1), 164.512(a)(1).); and

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

D. No HIPAA Business Associate Agreement or Relationship Between CDPH and Participant: This Agreement and the relationship it memorializes between CDPH and Participant do not constitute a business associate agreement or business associate relationship pursuant to 45 C.F.R. § 160.103 (definition of "business associate"). The basis for this determination is 45 C.F.R. § 160.203(c) (see, also, [HITECH Act, § 13421, sub. (a)].) [NOTE: See state laws and regulations listed in Attachment A]. Accordingly, this Agreement is not intended to nor at any time shall result in or be interpreted or construed as to create a business associate relationship between CDPH and Participant. By the execution of this Agreement, CDPH and Participant expressly disclaim the existence of any business associate relationship.

VI. Permitted Disclosures: The Participant and its workforce members and agents, shall safeguard the CalREDIE Data to which they have access to from unauthorized disclosure. The Participant, and its workforce members and agents, shall not disclose any CalREDIE Data for any purpose other than carrying out the Participant's obligations under the statutes and regulations set forth in Attachment A, or as otherwise allowed or required by state or federal law.

VII. Permitted Use: The Participant, and its workforce members and agents, shall safeguard the CalREDIE Data to which they have access to from unauthorized use. The Participant, and its workforce members and agents, shall not use any CalREDIE Data for any purpose other than carrying out the Participant's obligations under the statutes and regulations set forth in Attachment A or as otherwise allowed or required by state or federal law.

VIII. Restricted Disclosures and Uses:

A. [Reserved.]

IX. Safeguards: Participant shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of CalREDIE Data. The Participant 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 Participant'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 X, Security, below. Participant shall provide CDPH with Participant's current and updated policies.

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

A. 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 in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, and/or NIST 800-53 (version 4 or subsequent approved versions) which sets forth guidelines for automated information systems in Federal agencies; and

B. 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 CalREDIE Data from breaches and security incidents.

XI. Security Officer: The Participant shall designate a Security Officer to oversee its compliance with this Agreement and for communicating with CDPH on matters concerning this Agreement. Such designation is set forth in Attachment B, which is made a part of this Agreement by this reference.

XII. Training: The Participant shall provide training on its obligations under this Agreement, at its own expense, to all of its workforce members who assist in the performance of Participant's obligations under this Agreement, or otherwise use or disclose CalREDIE Data.

A. The Participant shall require each workforce member who receives training to receive and sign a certification, indicating the workforce member's name and the date on which the training was completed.

B. The Participant shall retain each workforce member's written certifications for CDPH inspection for a period of three years following contract termination.

XIII. Workforce member Discipline: Participant shall discipline such workforce members who intentionally violate any provisions of this Agreement, including, if warranted, by termination of employment.

XIV. Participant Breach and Security Incident Responsibilities:

A. Notification to CDPH of Breach or Security Incident: The Participant shall notify CDPH **immediately by telephone call plus email or fax** upon the discovery of a breach (as defined in this Agreement), **or** within **twenty-four (24) hours by email 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 XIV(G), below. If the breach or security incident occurs after business hours or on a weekend or holiday and involves CalREDIE Data in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH IT Service Desk at the telephone numbers listed in Section XIV(G) below. For purposes of this Section, breaches and security incidents shall be treated

as discovered by Participant as of the first day on which such breach or security incident is known to the Participant, or, by exercising reasonable diligence would have been known to the Participant. Participant 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 a workforce member or agent of the Participant.

Participant shall take:

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

2. any action pertaining to a breach required by applicable federal or state laws, including, specifically, California Civil Code section 1798.29.

B. Investigation of Breach: The Participant shall immediately investigate such breach or security incident, and within seventy-two (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 CalREDIE Data and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the CalREDIE Data, or to whom it is known (or reasonably believed) to have had the CalREDIE Data improperly disclosed to them; and

3. a description of where the CalREDIE Data is known or believed to have been improperly used or disclosed; and

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

5. whether Civil Code section 1798.29 or any other federal or state laws requiring individual notifications of breaches have been triggered.

C. Written Report: The Participant 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 (5) 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 Participant is considered only

a custodian and/or non-owner of the CalREDIE Data, Participant 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 laws. The CDPH Privacy Officer shall approve, in writing, the time, manner and content of any such notifications, prior to the transmission of such notifications to the individual(s); or

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

E. Submission of Sample Notification to California Attorney General: If notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29, Participant shall, at its sole expense, and at the sole election of CDPH, either:

1. electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the California Attorney General pursuant to the format., content and timeliness provisions of Section 1798.29, subdivision (e). Participant shall inform the CDPH Privacy Officer of the time, manner and content of any such submissions, prior to the transmission of such submissions to the Attorney General; or

2. cooperate with and assist CDPH in its submission of a sample copy of the notification to the California Attorney General.

F. Public Statements: Participant shall cooperate with CDPH in developing content for any public statements regarding Breaches or Security Incidents related to Participant and shall not provide any public statements without the express written permission of CDPH. Requests for public statement(s) by any non-party about a breach or security incidents shall be directed to the CDPH Program Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XIV(G), below.

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

[This space intentionally left blank – Continued on next page.]

CDPH Program Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer (and CDPH IT Service Desk)
CalREDIE Help Desk California Department of Public Health Division of Communicable Disease Control Communicable Disease Emergency Response Program CalREDIE Help Desk P.O. Box 997377, MS 7325 Sacramento, CA 95899-7377 California Department of Public Health Email: CalREDIEHelp@cdph.ca.gov Telephone: (866) 866-1428	**Privacy Officer** Privacy Office, c/o Office of Legal Services California Department of Public Health 1415 L Street, Suite 500 Sacramento, CA 95814 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	**Chief Information Security Officer** Information Security Office California Department of Public Health P.O. Box 997413, MS 6300 Sacramento, CA 95899-7413 Email: cdph.infosecurityoffice@cdph.ca.gov Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

XV. CDPH Breach and Security Incident Responsibilities: CDPH shall notify Participant immediately by telephone call plus email or fax upon the discovery of a breach (as defined in this Agreement), or within twenty-four (24) hours by email or fax of the discovery of any security incident (as defined in this Agreement) that involves CalREDIE Data that was created or collected by Participant in the CalREDIE System. Notification shall be provided by CDPH to the Participant Representative, using the contact information listed in Attachment B, which is made a part of this Agreement by this reference. For purposes of this Section, breaches and security incidents shall be treated as discovered by CDPH as of the first day on which such breach or security incident is known to CDPH, or, by exercising reasonable diligence would have been known to CDPH. CDPH 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 a workforce member or agent of CDPH.

A. Participant Contact Information: To direct communications to the Participant's breach/security incident response staff, CDPH shall initiate contact as indicated by Participant in Attachment B. Participant's contact information must be provided to CDPH prior to execution of this Agreement. Participant reserves the right to make changes to the contact information in Attachment B. Said changes shall not require an amendment to this Agreement.

XVI. Compliance with California Health and safety Code Section 121022(h): CDPH and Participant shall comply, when required, with California Health and safety Code Section 121022, subdivision (h), which provides as follows: "Any potential or actual breach of confidentiality of HIV-related public health records shall be investigated by the local health officer, in coordination with the department, when appropriate. The local health officer shall immediately report any evidence of an actual breach of confidentiality of HIV-related public health records at a city or county level to the department and the appropriate law enforcement agency. The department shall investigate any potential or actual breach of confidentiality of HIV-related public health records at the state level, and shall report any evidence of such a breach of confidentiality to an appropriate law enforcement agency."

XVII. Indemnification: Each party hereby agrees to indemnify, hold harmless, and defend the other party from and against any and all claims, losses, liabilities, damages, costs and other expenses (including attorneys' fees) that result from or arise directly or indirectly out of or in connection with any negligent act or omission or willful misconduct of Participant or CDPH, its officers, workforce members or agents relative to the CalREDIE Data, including, without limitation, any violations of Participant's or CDPH's responsibilities under this Agreement.

XVIII. Term of Agreement: Unless otherwise terminated earlier in accordance with the provisions set forth herein, this Agreement shall remain in effect for three (3) years after the latest signature date in the signature block below. After three (3) 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. 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 XIX, below.

XIX. Termination for Cause:

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

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

XX. 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 CalREDIE Data. Upon CDPH's request, Participant 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 thirty (30) days written notice in the event:

A. Participant does not promptly enter into negotiations to amend this Agreement when requested by CDPH pursuant to this Section, or

B. Participant does not enter into an amendment providing assurances regarding the safeguarding of CalREDIE 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 CalREDIE Data.

XXI. Assistance in Litigation or Administrative Proceedings: Each party shall make itself and any workforce members or agents assisting in the performance of obligations under this Agreement available to the other party at no cost to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced based upon claimed violation of laws relating to security and privacy, which involve inactions or actions by CDPH or Participant, except where CDPH and Participant or their workforce members or agents are a named adverse party.

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

XXIII. Transfer of Rights: Participant has no right and shall not 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.

XXIV. No Third-Party Beneficiaries: Nothing express 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 Participant, any rights, remedies, obligations or liabilities whatsoever.

XXV. 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.

XXVI. Survival: The respective rights and obligations of Participant under Sections VII, IX, XIV, and XVII of this Agreement shall survive the termination or expiration of this Agreement.

XXVII. Attachments: The parties mutually agree that the following specified Attachments are part of this Agreement:

A. Attachment A: State Law Authority for: (1) Use and Disclosure of CalREDIE Data; and, (2) Application of HIPAA preemption exception for public health (45 C.F.R. § 160.203(c)).

B. Attachment B: Participant Contact Information.

XXVIII. Entire Agreement: This Agreement, including all attachments, constitutes the entire agreement between CDPH and Participant. 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.

XXIX. 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.

XXX. Choice of Law and Venue: The laws of the state of California will govern any dispute from or relating to this Agreement. The parties submit to the exclusive jurisdiction of the state of California and federal courts for or in Sacramento and agree that any legal action or proceeding relating to the Agreement may only be brought in those courts.

XXXI. Signatures:

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

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

Dawn Rowe Name (Print)	_____ Name (Sign)
Chair, Board of Supervisors Title [Health Officer (or other authorized official)]	_____ Date
San Bernardino County Department of Public Health County/City Name (Print)	

On behalf of the **Department of Public Health**, the undersigned individual(s) hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

_____ James Watt, M.D., M.P.H. Chief, Division of Communicable Disease Control California Department of Public Health	_____ Date

Attachment A

State Law Authority for:

(1) Use and Disclosure of CalREDIE Data; and,

(2) Application of HIPAA preemption exception for public health (45 C.F.R. § 160.203(c).

General Authority:

1) Information Practices Act
    a. CA Civil Code section 1798.24(e) An agency shall not disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains unless the information is disclosed, as follows: (e) To a person, or to another agency where the transfer is necessary for the transferee agency to perform its constitutional or statutory duties, and the use is compatible with a purpose for which the information was collected and the use or transfer is accounted for in accordance with Section 1798.25. With respect to information transferred from a law enforcement or regulatory agency, or information transferred to another law enforcement or regulatory agency, a use is compatible if the use of the information requested is needed in an investigation of unlawful activity under the jurisdiction of the requesting agency or for licensing, certification, or regulatory purposes by that agency.

Specific Authority:

1) Functions and Duties of the Department of Public Health, Reportable Diseases and Conditions from Providers and Labs
    a. California Health and Safety Code section 120130
        i. Subdivision (a): The department shall establish a list of reportable diseases and conditions. For each reportable disease and condition, the department shall specify the timeliness 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…Those diseases listed as reportable shall be properly reported as required to the department by the health officer.
        ii. Subdivision (g): Commencing July 1, 2009, or within one year of the establishment of a state electronic laboratory reporting system, whichever is later, a report generated pursuant to this section, or Section 121022, by a laboratory shall be submitted electronically in a manner specified by the department. The department shall allow laboratories that receive incomplete patient information to report the name of the provider who submitted the request to the local health officer.
    b. California Code of Regulations. Title 17. Public Health Division 1. State Department of Health Services Chapter 4. Preventive Medical Service
        i. Article 1 Reporting:
            1. Section 2500: Provider Reporting of Diseases and Conditions to the Local Health Officer and Confidentiality of Reports
            2. Section 2501: Investigation of a Reported Case, Unusual Disease, or Outbreak of Disease
            3. Section 2502: Reports by Local Health Officer to State Department of Public Health.
            4. Section 2505: Notification of Diseases and Conditions by Laboratories

2) HIV Specific Laws related to Reporting, Surveillance Sharing and Confidentiality, Penalties for Disclosure:
    a. Health and Safety Code section 121022, HIV Reporting by Providers and Labs
    b. Health and Safety Code section 121023, Lab Reporting of CD4+ T-Cell test results
    c. Health and Safety Code section 121025 (b) disclosure of HIV records between state and local public health agencies for 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.
    d. California Code of Regulations. Title 17. Public Health Division 1. State Department of Health Services Chapter 4. Preventive Medical Service
        i. Article 3.5, Reporting of HIV, Subarticle 1 and Subarticle 4, Sections: 2641.5-2643.20
    e. California HIV/AIDS-Specific Statutes Pertaining to Confidential Public Health Records and Penalties for Disclosures (this list is not comprehensive):
        i. All HIV/AIDS case reports and any HIV/AIDS related information collected or maintained by CDPH (or its agents or contractors) or a local health department or agency (or its agent or contractors), 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.
        ii. HSC section 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 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-$25,000 plus court costs as provided by HSC 121025(e)(2). Any willfully, malicious, or negligent disclosure of information contained in a public health record in violation of state law that results in economic, bodily, psychological harm to a 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 section 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 section 121025(e)(4)]. Each disclosure in violation of California law is a separate, actionable offense [HSC section 121025(e)(5)].

Attachment B

Participant Contact Information

The following contact information must be provided prior to execution of this Agreement.

Participant Program Manager	**Participant Privacy Officer**	**Participant Chief Information Security Officer (and IT Service Desk Telephone)**
Name: Diana Ibrahim Address: 451 E. Vanderbilt Way San Bernardino, CA, 92415 Email: Diana.Ibrahim@dph.sbcounty.gov Telephone: (909) 387-6337	Name: Matthew Higgins Address: 451 E. Vanderbilt Way San Bernardino, CA, 92415 Email: Matthew.Higgins@DPH.sbcounty.gov Telephone: (909) 659-6064	Name: Robert Pittman Address: 670 E. Gilbert St. San Bernardino, CA, 92415 Email: Robert.Pittman@isd.sbcounty.gov Telephone: (909) 388-5510 IT Service Desk Telephone: (909) 884.4484