CalCONNECT System for California Connected
Data Use and Disclosure Agreement

This CalCONNECT System ("CalCONNECT") Data Use and Disclosure Agreement ("Agreement") for the California Connected Program sets forth the information privacy and security requirements that Humboldt County DHHS - Public Health ("Participant"), and the California Department of Public Health ("CDPH") are obligated to follow with respect to all CalCONNECT Data (as defined herein) collected or created within the CalCONNECT System. Participant will have access to the CalCONNECT System managed by CDPH and will use it for surveillance and control of Contagious, Infectious, Communicable or Reportable Diseases and Conditions (as defined herein) in Humboldt County DHHS - Public Health . By entering into this Agreement, CDPH and Participant agree to protect the privacy and provide for the security of all CalCONNECT Data in compliance with all state and federal laws applicable to the CalCONNECT Data. Permission to receive, use and disclose CalCONNECT Data requires execution of this Agreement that describes the terms, conditions, and limitations of Participant's collection, use, and disclosure of the CalCONNECT Data.

I. Supersession: This Agreement supersedes any prior CalCONNECT 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 CalCONNECT Data in violationof 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 CalCONNECT System only.

B. CalCONNECT System Data: "CalCONNECT System Data" means data in the CalCONNECT System including demographic, epidemiologic (including clinical information, risk factor information, exposure information, information on Cases and Contacts, inclusive of long term conditions which they may be experiencing and laboratory test result information), as well as administrative information on Contagious, Infectious, Communicable or Reportable Diseases and Conditions collected for contact tracing, case investigation, and for examining the causes of the communicable diseases and conditions, to ascertain the nature of the disease or condition and to prevent its spread.

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

    a. California Reportable Disease Information Exchange (CalREDIE) System, which includes:

        i. 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.

        ii. Laboratory Test and Result information required by Title17 of the CCR sections 2505 and 2641.5 - 2643.20.

        iii. Communicable Disease Control Report Forms (requiredfor specific diseases and conditions that are mandated by state laws and regulations to be reported by healthcare providers and laboratories to local healthofficers), including cases of the Contagious, Infectious, Communicable or Reportable Diseases and Conditions.

    b. California Connected Activities,may include:

        i. Demographic data of Cases and Contacts;

        ii. Information obtained through interviews with Cases and Contacts, including but not limited to, self-reported health information, long term symptoms, demographic information, location and location history information, risk factor information, laboratory test results, and other personal information as defined by Civil Code section 1798.3; and

        iii. Records of communications with Cases and Contacts which contain personal informationas defined by Civil Code section 1798.3, including but not limited to, phone call recordings, SMS (text) messages, call logs, and tracking sheets.

2. CalCONNECT Data specifically excludes the following information:

    a. Mental Health Information unrelated to the Contagious, Infectious, Communicable or Reportable Diseases and Conditions being monitored;

    b. California Supplemental Pay Sick Leave (“CSPSL”) aka (“Backpay”);

    c. Sincerely held religious beliefs, practices, or observances which include moral or ethical beliefs, and

d. Political, sociological, or philosophical views affiliated with any individual.

C. California Connected: "California Connected" means the State of California program launched in May 2020 for Contact Tracing, Communicable or Reportable Disease surveillance and response, which was expanded to include Contagious, Infectious, Communicable or Reportable Diseases and Conditions and public awareness related to Contagious, Infectious, Communicable or Reportable Diseases and Conditions.

D. "Contagious, Infectious, Communicable or Reportable Diseases and Conditions" means:

1. the same definition as set forth in Title 17 of the CCR section 2500 subsection (8), "… an illness due to a specific microbiological or parasitic agent or its toxic products which arises through transmission of that agent or its products from an infected person, animal, or inanimate reservoir to a susceptible host, either directly or indirectly through an intermediate plant or animal host, vector, or the inanimate environment;"

2. the diseases listed in Title 17 of the CCR section 2502 subsection (b);

3. the reportable conditions listed in Title 17 of the CCR section 2505 which requires labs to report laboratory testing results, including molecular and pathologic results, suggestive of diseases of public health importance; and

4. Contagious, Infectious, Communicable or Reportable diseases and conditions indicated by a local health officer to CDPH, for which CDPH has determined will qualify under this category, permitting CDPH to take measures as necessary to ascertain the nature of the disease or condition and prevent its spread under HSC section 120140.

E. Contact Tracing: "Contact Tracing" means the process of tracking Contagious, Infectious, Communicable or Reportable Diseases and Conditions as it spreads from person to person with the goal of halting transmission.

F. Cases: "Cases" means persons with a suspected or confirmed case, or a person who has been exposed to an animal with a suspected or confirmed case of a Contagious, Infectious, Communicable or Reportable Diseases and Conditions under investigation in California.

G. Contacts: "Contacts" means persons in California who may have been in contact with, interacted with or were otherwise exposed to a Case.

H. Disclosure: "Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of information obtained from the CalCONNECT system, related to any individual containing Personal Identifying Information ("PII") or Protected Health Information ("PHI").

I. Security Incident: "Security Incident" means:

1. an attempted breach;

2. the attempted or successful modification or destruction of CalCONNECT Datain the CalCONNECT 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 CalCONNECT System that negatively impacts the confidentiality, availability or integrity of CalCONNECT Data, or hinders or makes impossible the receipt, collection, creation, storage, transmission or use of CalCONNECT Data in the CalCONNECT System.

J. Use: "Use" means the sharing, employment, application, utilization, examination, or analysis of information for any purposes including publication. Please note this list is not exhaustive.

K. 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.

L. [Reserved.]

III. Background and Purpose: The CalCONNECT System is an online database that maintains information, originally collected by local health department or CDPH staff or their agents, related to Contagious, Infectious, Communicable or Reportable Diseases and Conditions. It was initially established in response to the 2020 worldwide outbreak of COVID-19; and has since been expanded for use to collect information on any Contagious, Infectious, Communicable or Reportable Diseases and Conditions that CDPH wishes to take measures as necessary on to ascertain the nature of the disease and prevent its spread. The purpose of this database is to improve the efficiency of disease surveillance and response activities and the early detection of public health events through the collection of more complete and timely surveillance information on a state-wide basis. CalCONNECT is a secure, web-based electronic solution for state departments and local health departments to maintain information to allow them to interview Cases and Contacts, identify the individuals they have interacted with collect their conditions and symptoms and notify those contacts to evaluate whether they need to isolate or quarantine or whether any additional measures are necessary or appropriate. CalCONNECT is an integral part of the overall California public health response strategy to Contagious, Infectious, Communicable or Reportable Diseases and Conditions as a database resource to adequately implement statewide contact tracing through both state departments and local health departments.

IV. Legal Authority for Collection, Use and Disclosure of CalCONNECT Data: The legal authority for CDPH and Participant to collect, use and disclose CalCONNECT Data is setforth 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 CalCONNECT 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, ofthe Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111–5, 123 Stat. 265–66)). The CalCONNECT 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. § 164.105 (a)(2)(i)(B).) The legal basis for this determination is as follows:

1. The CalCONNECT 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. §§ 160.105(a)(2)(iii)(D); 160.103 (definition of "coveredentity")); 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. CalCONNECT Data Use and Disclosure Permitted by HIPAA: To the extent a disclosure or use of CalCONNECT 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 CalCONNECT 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 ofpublic 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." (Title 45 C.F.R. §§ 164.502 (a)(1)(vii), 164.512(a) (1).) and,

4. Other, non-public health-specific provisions of HIPAA may also provide the legal basis for all or specific CalCONNECT 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 Title 45, CFR, Part 160.103 (definition of "business associate"). The basis for this determination is Section 160.203(c) of Title 45 of the Code of Federal Regulations (see, also, [HITECH Act, § 13421, subdivision. (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 acknowledges that once data is entered into the CalCONNECT System, the Participant and its workforce members and agents shall safeguard the CalCONNECT Data to which they have access from unauthorized disclosure. The Participant, and its workforce members and agents, shall not access or disclose any CalCONNECT Data for any purpose other than carrying out the Participant's obligations under this Agreement or the statutes and regulations set forth in Attachment A, or as otherwise allowed or required by state or federal law. When Cases and Contacts cross into another county's jurisdiction, the Participant shall be permitted to disclose CalCONNECT Data with the local health department of that county's jurisdiction. Any such disclosure of CalCONNECT Data shall be limited to the minimum necessary, to the extent practicable, in carrying out the Participant's obligations under this Agreement or as otherwise allowed or required by state or federal law. Requests for release of data through generated reports created by CDPH will be disclosed to Participant when permissible. Otherwise, the Participant acknowledges the necessity of safeguarding the CalCONNECT Data in accordance with state and federal laws.

Should any additional disclosures not already addressed in this section, be requested by the Participant or its workforce members and agents, these requests must be presented to the California Connected Program and will require the approval of the Office of Legal Services at CDPH prior to any disclosure.

VII. Permitted Use: The Participant, and its workforce members and agents, shall safeguard the CalCONNECT Data to which they have access to from unauthorized use. The Participant, and its workforce members and agents, shall not use any CalCONNECT Data for any purpose other than carrying out the Participant's obligations under this Agreement or the statutes and regulations set forth in Attachment A, or as otherwise allowed or required by state or federal law. Any other use is strictly prohibited. Any such use of CalCONNECT Data shall be limited to the minimum necessary, to the extent practicable, in carrying out the Participant's obligations under this Agreement or as otherwise allowed or required by state or federal law. Participant shall collect no more than the minimum necessary amount of information necessary to perform its obligations as set forth in this Agreement. Further, should the Participant collect any CalCONNECT Data that may be protected by 42 CFR Part 2, a federal regulation that requires substance abuse disorder treatment providers to observe additional privacy and confidentiality restrictions with respect to patient records in the

CalCONNECT system, they must adhere to those stringent privacy protections which are more restrictive than HIPAA. Any and all violations may be grounds for removal from use of CalCONNECT at the election of CDPH.

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 CalCONNECT 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 CalCONNECT 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 CalCONNECT 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 CalCONNECT Data.

A. The Participant shall require each workforce member who receives training to receive a certificate of completion, indicating the workforce member's name and the date on which the training was completed. The content of the training in the Participant's Learning Management System (LMS) shall include an agreement for workforce member to comply with all applicable federal and state laws.

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

XIII. Workforce Member Discipline: Participant shall impose discipline that it deems appropriate (in its sole discretion) on such employees and other Participant workforce members under Participant's direct control who intentionally or negligently violate any provisions of this Agreement.

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 CalCONNECT Data inelectronic 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 CalCONNECT 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 CalCONNECT Data and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the CalCONNECT Data, or to whom it is known (or reasonably believed) to have had the CalCONNECT Data improperly disclosed to them; and

3. a description of where the CalCONNECT 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 CalCONNECT 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 Participantand

shall not provide any public statements without the express written permissionof 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.

CDPH Program Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer (and CDPH IT Service Desk)
Ryan Murphy, PHD, MPH Epidemiology Unit Chief Email: ryan.murphy@cdph.ca.gov Telephone: (510) 620-6718	**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 6302 Sacramento, CA 95899-7413 Email: CDPH.InfoSecurityOffice@cdph.ca.gov Telephone: IT Service Desk (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 CalCONNECT Data that was created or collected by Participant in the CalCONNECT 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. Term of Agreement: Unless otherwise terminated earlier in accordance with the provisions set forth herein, this Agreement shall remain in effect for a period of three (3) years as agreed upon by the Parties, 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 written notice. CDPH may also terminate this Agreement pursuant to Section XVIII, below.

XVIII. Termination for Cause:

A. Termination Upon Breach: A breach by either party of any provision of thisAgreement, as determined by CDPH or Participant, shall constitute a material breach of the Agreement and grounds for immediate termination of the Agreementby CDPH or Participant by providing written notice of such termination. 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 in writing 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 by providing written notice to the other party if the other party is found guilty of acriminal violation related to a violation of this Agreement. CDPH or Participant may terminate the Agreement by providing written notice to the other party 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.

XIX. 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 CalCONNECT 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 regardingthe safeguarding of CalCONNECT 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 CalCONNECT Data.

XX. 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, inthe event of litigation or administrative proceedings being commenced based upon claimed violation of laws relating to security and privacy, which involve inactions or actions byCDPH or Participant, except where CDPH and Participant or their workforce members or agents are a named adverse party.

XXI. 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 forall decisions made by Participant regarding the safeguarding of CalCONNECT Data.

XXII. 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.

XXIII. 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.

XXIV. 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.

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

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

B. Attachment B: Participant Breach and Security Incident Contact Information.

XXVII. 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.

XXVIII. 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.

XXIX. 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.

XXX. Signatures:

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

On behalf of Humboldt County DHHS - Public Health ("Participant"), 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.

Sofia Pereira

Public Health Director

Humboldt County DHHS - Public Health

529 I Street

Eureka, CA 95501

Approved as to Form (Optional):

By:

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.

Ryan Murphy, PhD MPH
Product Owner / Data Systems Manager
California Department of Public Health
850 Marina Bay Parkway, Building P
Richmond, CA 94804

Return Executed Agreement to:
Larissa Juarez
Office of Legal Services, California Department of Public Health
Larissa.Juarez@cdph.ca.gov

Attachment A

State Law Authority for Use and Disclosure of CDPH CalCONNECT Data; and Application of HIPAA preemption exception for public health (45 C.F.R. § 160.203(c)).

A. Legal Authority:

1. California Information Practices Act:

   a. California Civil Code section 1798.24, subdivision (i), provides in part as follows: “Anagency 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: Pursuant to a determination by the agency that maintains information that compelling circumstances exist that affect the health or safety of anindividual….”

2. California Health and Safety Code section 101085

3. California Health and Safety Code section 120125

4. California Health and Safety Code section 120130

5. California Health and Safety Code section 120140

6. California Health and Safety Code sections 120175 & 120175.5

7. California Health and Safety Code sections 121022-121035

8. Title 17. Public Health, Division 1. State Department of Health Services, Chapter 4. Preventative Medical Service, Article 1, Reporting, Sections: 2500, 2502, and 2505

9. Title 17. Public Health, Division 1. State Department of Health Services, Chapter 4. Preventative Medical Service, Article 3.5, Reporting of HIV, Sub Article 4, Sections: 2641.5-2643.20

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**
Name: Megan Blanchard	Name: Amy Cone	Name: Zachary Smith
Title: Director of Nursing	Title: Privacy Officer & Quality Assurance Manager	Title: HHS Deputy Director Information Services
Address 1: 529 I Street	Address 1: 507 F Street	Address 1: 507 F Street
Address 2:	Address 2:	Address 2:
City: Eureka	City: Eureka	City: Eureka
State, Zip Code: CA, 95501	State, Zip Code: CA, 95501	State, Zip Code: CA, 95501
Telephone: 707-362-1657	Telephone: 707-267-8847	Telephone: 707-362-1855
Fax:	Fax:	Fax:
E-mail: mblanchard@co.humboldt.ca.us	E-mail: acone@co.humboldt.ca.us	E-mail: zsmith@co.humboldt.ca.us