California Department of Public Health–Maternal, Child and Adolescent Health Division and the Injury and Violence Prevention Branch

Data Use and Disclosure Agreement

This Data Use Agreement (Agreement) is between the California Department of Public Health (specifically, the Maternal, Child and Adolescent Health Division (MCAH) and the Injury and Violence Prevention Branch (IVPB)) and County of Humboldt (COUNTY) and sets forth the information privacy and security requirements Recipient is obligated to follow with respect to all DATA from the National Fatality Review Case Reporting System (NFRCRS) disclosed to Recipient. The California Department of Public Health (CDPH) and Recipient desire to protect the privacy and provide for the security of the DATA pursuant to this Agreement, in compliance with state and federal laws applicable to the DATA.

I. Order of Precedence: With respect to information privacy and security requirements for all DATA, the terms and conditions of this Agreement shall take precedence over any conflicting terms or conditions set forth in any other agreement between Recipient and CDPH.

II. Effect on Lower Tier Transactions: The terms of this Agreement shall apply to all contracts, subcontracts, and subawards, and the information privacy and security requirements Recipient is obligated to follow with respect to DATA disclosed to Recipient pursuant to Recipient's agreement with CDPH. When applicable, Recipient shall incorporate the relevant provisions of this Agreement into each subcontract or subaward to its agents, subcontractors, or independent consultants.

III. Definitions: For purposes of the Agreement between Recipient and CDPH, the following definitions shall apply:

A. Breach: "Breach" means:

1. the unauthorized acquisition, access, use, or disclosure of DATA in a manner which compromises the security, confidentiality or integrity of the information; or

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

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

1. does not meet the definition of "public records" set forth in California Government Code section 7920.530, or is exempt from disclosure under any of the provisions of Section 7921.000, et seq. of the California Government Code or any other applicable state or federal laws; or

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

C. DATA: "DATA" means and refers to all identifiable and de-identified data collected to promote policy, programs, services and laws to prevent fetal, infant and child deaths at the local, state and national levels to better identify and address health disparities from the National Fatality Review Case Reporting System administered by the Maternal, Child and Adolescent Health Division (MCAH) and the Injury and Violence Prevention Branch (IVPB) at CDPH. Access will be granted to each county/city health

department as indicated through this Agreement for the purposes of assisting them with the analysis and reporting of California cases pertinent to their jurisdiction.

D. Disclosure: “Disclosure” means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

E. PCI: “PCI” means “personal information” and “confidential information” (as these terms are defined herein)

F. Personal Information: “Personal information” means information, in any medium (paper, electronic, oral) that:

1. directly or indirectly collectively identifies or uniquely describes an individual; or

2. 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, subdivision (g)(1) or (g)(2); or

5. meets the definition of “medical information” set forth in either California Civil Code section 1798.29, subdivision (h)(2) or California Civil Code section 56.05, subdivision (j); or

6. meets the definition of “health insurance information” set forth in California Civil Code section 1798.29, subdivision (h)(3); or

7. is protected from disclosure under applicable state or federal law.

G. Security Incident: “Security Incident” means:

1. an attempted breach; or

2. the attempted or successful unauthorized access or disclosure, modification or destruction of 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, Recipient’s system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of DATA; or

4. any event that is reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset, system, process, data storage, or transmission. Furthermore, an information security incident may also include an event that constitutes a violation or imminent threat of violation of information security policies or procedures, including acceptable use policies.

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

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

IV. No HIPAA Business Associate Agreement or Relationship Between the Parties: This Agreement and the relationship it memorializes between the Parties does not constitute a business associate agreement or business associate relationship pursuant to Title 45, C.F.R., 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)].). 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 the Parties.

V. Background and Purpose: CDPH administers a broad range of public and clinical health programs that provide health care and preventative services to Californians, including those programs within the Injury and Violence Prevention Branch (IVPB) and the Maternal, Child and Adolescent Health Division (MCAH). Under legislative mandate, CDPH is required to perform special investigation studies of the sources of morbidity and mortality, and the effects of localities, employments, conditions and circumstances on the public health, and perform other duties as may be required in procuring information for state and federal agencies regarding the effects of these conditions on the public health. CDPH may conduct surveillance for child fatalities in California using data from multiple sources, including state level data sources and data obtained by local child death review teams (CDRTs). The Fatal Child Abuse and Neglect Surveillance (FCANS) Program, now called the California Child Fatality Surveillance System (CCFSS), was established in July 2000 to allow CDPH to conduct surveillance on child fatalities. CDPH chose to administer the National Fatality Review Case Reporting System in order to conduct surveillance on child fatalities for California. Two State programs (i.e., IVPB and MCAH) will primarily be involved with granting data access and intend on assisting county and city health departments by providing them with direct access to this National Fatality Review Case Reporting System, which is managed by CDPH for analysis and reporting of California cases pertinent to their jurisdiction. CDPH is providing access to a federal government database for the efficiency of collecting, reporting and reviewing death information by counties, cities, and local health jurisdictions.

VI. Disclosure Restrictions: Recipient and its employees, agents, and subcontractors shall protect from unauthorized disclosure any DATA. Recipient shall not disclose, except as otherwise specifically permitted by this Agreement between Recipient and CDPH, any DATA to anyone other than CDPH personnel or programs without prior written authorization from the CDPH Program Contract Manager, except if disclosure is required by State or Federal law.

VII. Legal Authority: The legal authority for CDPH and the Local Health Departments to collect, create, access, use, and disclose DATA are Health and Safety Code (HSC) §§ 100325-100335, 123650 – 123660, and 131230, and Penal Code § 11174.34. Under those sections, CDPH is responsible for developing a plan to identify causes of mortality and morbidity in California, and to study recommendations on the reduction of mortality and morbidity in California.

VIII. Use Restrictions: Recipient and its employees, agents, and subcontractors shall not use any DATA for any purpose other than performing Recipient's obligations under this Agreement. Additionally, CDPH

acknowledges that there are only two (2) levels of access that CDPH staff will consider as being the most appropriate level of access for which a Recipient may be granted: as a Data Analyst or Case Reporter. Depending on the level of access, Recipient may view identifiable and/or de-identified DATA pertaining to their own county, but no DATA pertaining to other counties. In accordance with the National CFRP User Manual version 6.0, a Data Analyst will have the ability to download DATA (identified or de-identified) for their team, which will pertain to their own county, only after authorization from CDPH Administrators have been granted, and from there, be able to create standardized reports. However, Case Reporters will only have the ability to enter, edit and print case information for their team/county, as well as conduct searches and create standardized reports.

IX. Safeguards: Recipient shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of DATA, including electronic or computerized DATA. At each location where DATA exists under Recipient's control, 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 Recipient's operations and the nature and scope of its activities in performing this Agreement, and which incorporates the requirements of Section X, Security, below. Recipient shall provide CDPH with Recipient's current and updated policies within five (5) business days of a request by CDPH for the policies.

X. Security: Recipient shall take any and all steps reasonably necessary to ensure the continuous security of all computerized data systems containing DATA. These steps shall include, at a minimum, the following:

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 5 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 either 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 the DATA from breaches and security incidents.

XI. Security Officer: At each place where DATA is located, Recipient shall designate a Security Officer to oversee its compliance with this Agreement and to communicate with CDPH on matters concerning this Agreement.

XII. Training: 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 Recipient's obligations under Recipient's agreement with CDPH, including this Agreement, or otherwise use or disclose DATA.

A. Recipient shall require each employee who receives training to certify, either in hard copy or electronic form, the date on which the training was completed.

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

C. Recipient shall provide CDPH with its employee's certifications within five (5) business days of a request by CDPH for the employee's certifications.

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

XIV. Breach and Security Incident Responsibilities:

A. Notification to CDPH of Breach or Security Incident: Recipient shall notify CDPH **immediately by telephone call plus email** upon the discovery of a breach (as defined in this Agreement), and **within twenty-four (24) hours by email** of the discovery of any security incident (as defined in this Agreement), unless a law enforcement agency determines that the notification will impede a criminal investigation, in which case the notification required by this section shall be made to CDPH immediately after the law enforcement agency determines that such notification will not compromise the investigation. Notification shall be provided to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XI (F), below. If the breach or security incident is discovered after business hours or on a weekend or holiday and involves DATA in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH Information Security Office at the telephone numbers listed in Section XI(F), below. For purposes of this Section, breaches and security incidents shall be treated as discovered by Recipient as of the first day on which such breach or security incident is known to Recipient, or, by exercising reasonable diligence would have been known to Recipient. Recipient shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee or agent of Recipient.

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 and Security Incidents: Recipient shall immediately investigate such breach or security incident. As soon as the information is known and subject to the legitimate needs of law enforcement, Recipient shall inform the CDPH Program Contract 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 disclosure or access 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 DATA and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the DATA, or to whom it is known or reasonably believed to have had the DATA improperly disclosed to them; and

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

4. a description of the probable and proximate 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: Recipient shall provide a written report of the investigation to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer as soon as practicable after 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 complete, 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 or further disclosure of data regarding 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 Recipient is considered only a custodian and/or non-owner of the 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 laws. Recipient shall inform the CDPH Privacy Officer of 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. Submission of Sample Notification to Attorney General: If notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29, and regardless of whether Recipient is considered only a custodian and/or non-owner of the DATA, Recipient 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 Attorney General pursuant to the format, content and timeliness provisions of Section 1798.29, subdivision (e). Recipient 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 Attorney General.

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

CDPH Program Contract Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer
Renay Bradley Chief, Epidemiology, Surveillance, & Evaluation Section; Injury and Violence Prevention Branch Email: renay.bradley@cdph.ca.gov Telephone: (279) 213-1501 Christopher Borges State SIDS/FIMR Coordinator Perinatal Clinical Programs Section Maternal, Child and Adolescent Health Division Email: Christopher.Borges@cdph.ca.gov Telephone: (279) 944-9038	Privacy Officer Privacy Office Office of Legal Services California Dept. of Public Health P.O. Box 997377, MS 0506 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office California Dept. of Public Health P.O. Box 997377, MS6302 Sacramento, CA 95899-7413 Email: CDPH.InfoSecurityOffice@cdph.ca.gov Telephone: (855) 500-0016

XV. Documentation of Disclosures for Requests for Accounting: Recipient shall document and make available to CDPH or (at the direction of CDPH) to an Individual such disclosures of DATA, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of personal information as required by Civil Code section 1798.25, or any applicable state or federal law.

XVI. Requests for DATA by Third Parties: Recipient and its employees, agents, or subcontractors shall promptly transmit to the CDPH Program Contract Manager all requests for disclosure of any DATA requested by third parties to the agreement between Recipient and CDPH (except from an Individual for an accounting of disclosures of the individual's personal information pursuant to applicable state or federal law), unless prohibited from doing so by applicable state or federal law.

XVII. Audits, Inspection and Enforcement: CDPH may inspect the facilities, systems, books and records of Recipient to monitor compliance with this Agreement. Recipient shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the CDPH Program Contract Manager in writing.

XVIII. Termination for Cause:

A. Termination upon Breach: A breach by 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 Recipient 30 days to cure the breach, or CDPH may have the option to terminate access immediately to the Recipient.

B. Judicial or Administrative Proceedings: 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

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 Recipient has violated any security or privacy laws is made in any administrative or civil proceeding in which Recipient is a party or has been joined.

XIX. Amendment: The parties acknowledge that federal and state laws regarding information security and privacy rapidly evolve, 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 DATA. The parties agree to promptly enter into negotiations concerning an amendment to this Agreement consistent with new standards and requirements imposed by applicable laws and regulations.

XX. Assistance in Litigation or Administrative Proceedings: Recipient shall make itself and any subcontractors, workforce employees or agents assisting Recipient in the performance of its obligations under the agreement between Recipient and CDPH, available to CDPH at no cost to CDPH to testify as witnesses, 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 Recipient, except where Recipient or its subcontractor, workforce employee or agent is a named adverse party.

XXI. 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 Recipient and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

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

XXIII. Survival: If Recipient does not return or destroy the DATA upon the completion or termination of the Agreement, the respective rights and obligations of Recipient under Sections IX, X, and XIV of this Agreement shall survive the completion or termination of the agreement between Recipient and CDPH.

XXIV. 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.

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

XXV. Signatures:

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

On behalf of Recipient, the undersigned individual hereby attests that they are authorized to enter into this Agreement and agrees to abide by and enforce all the terms specified herein.

Sofia Pereira
(Name of Representative of Recipient)

Public Health Branch Director
(Title)

(Signature) (Date)

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

Mari Taylan
(Name of CDPH Representative)

Chief, MCAH Perinatal Clinical Programs and LHJ Support Section
(Title)

(Signature) (Date)

Attachment 1

Recipient Breach and Security Incident Contact Information.

The following Recipient contact information must be included in the executed Agreement

Recipient Program Manager	**Recipient Privacy Officer**	**Recipient Chief Information Security Officer (and IT Service Desk)**
Megan Blanchard	Jimmy Cookman	Scott Irving
Director of Public Health Nursing	Compliance and Quality Assurance Administrator	IT Division Director
908 7th Street	507 F Street	825 5th Street
[Address 2]	[Address 2]	[Address 2]
Eureka	Eureka	Eureka
CA, 95501	CA, 95501	CA, 95501
707-362-1657	707-572-7727	707-268-3674 or 707-362-6361 IT Service Desk 707-441-5555
707- 268-8495	[Fax]	[Fax]
mblanchard@co.humboldt.ca.us	jcookman@co.humboldt.ca.us	sirving@co.humboldt.ca.us