California Integrated Vital Records System (Cal-IVRS)
Local Health Department Participant Agreement

This California Integrated Vital Records System (Cal-IVRS) Data Privacy and Security Agreement (Agreement) sets forth the data privacy and security requirements that Nevada County Public Health Department [name of local health department] (Participant), and the California Department of Public Health (CDPH) are obligated to follow with respect to all Cal-IVRS Data (as defined herein). By entering into this Agreement, Participant and CDPH agree to protect the privacy and provide for the security of Cal-IVRS Data in compliance with all applicable state and federal laws concerning the Cal-IVRS Data. Permission for Participant to collect, create, access, use and disclose Cal-IVRS Data requires execution of this Agreement by Participant and CDPH.

I. Supersession: This Agreement supersedes any prior Cal-IVRS Agreement, or other agreement concerning Cal-IVRS Data, 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 Cal-IVRS 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 Integrated Vital Records System (Cal-IVRS), only.

B. Cal-IVRS Data : "Cal-IVRS Data" means: All data collected in, or created in, the following CDPH information technology systems/databases:

1. Vital Records Business Intelligence System (VRBIS).

2. Electronic Birth Registration System (EBRS).

3. Electronic Death Registration System (EDRS).

4. Fetal Death Registration System (FDRS).

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

D. Security Incident: "Security Incident" means:

1. An attempted breach.

2. The attempted or successful modification or destruction of Cal-IVRS Data in the California Integrated Vital Records 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 Integrated Vital Records System that negatively impacts the confidentiality, availability or integrity of Cal-IVRS Data, or hinders or makes impossible the receipt, collection, creation, storage, transmission or use of Cal-IVRS Data in the Cal-IVRS System.

E. Use: "Use" means the sharing, employment, application, utilization, examination, or analysis of Cal-IVRS Data.

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 CDPH and its Director, designated in statute as the State Registrar, pursuant to Division 102 of the California Health and Safety Code (H&SC), is charged with the duties of registering, maintaining, indexing and issuing certified copies of all California Birth, Death, and Fetal Death records. As part of these activities, the State Registrar operates the VRBIS, EBRS, EDRS, and FDRS databases. Responsibilities set forth in H&SC section 102247 and 102249 provide legislative direction to the State Registrar to develop and maintain an automation system for vital event registration, develop and maintain public health data bases, build a data system that will support policy analysis and program decisions at all levels, be useful to health care providers, local and community agencies, and the state to ultimately benefit consumers of health care services. VRBIS, EBRS, EDRS, and FDRS are necessary components to fulfilling these responsibilities.

A. VRBIS is a secure, web based electronic solution for the State Registrar to store California's vital records data and to permit Local Health Departments and others to access such data for purposes allowed under California statute, such as epidemiologic analysis, surveillance, and program evaluation, following all applicable laws and regulations concerning vital record data.

B. EBRS, EDRS, and FDRS are secure, web based electronic birth, death, and fetal death registration databases maintained by the State Registrar. Access to EBRS, EDRS, and FDRS is limited to statutorily defined record preparers, such as hospitals (section 102405,) funeral homes (sections 102780 and 102795,) and coroners (102850 – 102870,) as well as local registrars and the State Registrar, required by statute to register and preserve birth, death, and fetal death certificates. In EBRS, EDRS, and FDRS, record preparers enter certificate data into the registration database and electronically submit completed records to the local registrar to be registered. Once records are registered in EBRS, EDRS, and FDRS, record data are transmitted to VRBIS.

IV. Legal Authority: The legal authority for CDPH and Participant to collect, create, access, use and disclose Cal-IVRS Data is set forth in Attachment A to this Agreement, which is made part of this Agreement by this reference.

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

A. CDPH and Cal-IVRS 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 Cal-IVRS 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. § 164.504(c)(3)(iii).) The legal basis for this determination is as follows:

1. The Cal-IVRS 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 "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. § 60.203(c) [HITECH Act, § 13421, sub. (a)].) [NOTE: See State laws and regulations listed in Attachment A.

B. CDPH is a "Public Health Authority": CDPH is 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. Cal-IVRS Data Use and Disclosure Permitted by HIPAA: To the extent a disclosure or use of Cal-IVRS Data may also be considered a disclosure or use of "Protected Health Information" (PHI) of an individual, as that term is defined in part 160.103 of Title 45, Code of Federal Regulations, the following Privacy Rule provisions apply to permit such Cal-IVRS 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. § 60.203(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 Cal-IVRS 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 part 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 and its workforce members and agents, shall safeguard the Cal-IVRS Data to which they have access to from unauthorized disclosure. The Participant, and its workforce members and agents, shall not disclose any Cal-IVRS 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 Cal-IVRS Data to which they have access to from unauthorized use. The Participant, and its workforce members and agents, shall not use any Cal-IVRS 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. Notwithstanding the foregoing, inter-jurisdictional data may only be used in accordance with the following:

A. Permitted Use of Inter-jurisdictional Data: CDPH participates in the State and Territorial Exchange of Vital Events. As a participating state, CDPH receives data about births and deaths of California residents occurring in other states and territories. The VRBIS system makes this data available for use by local public health agencies. As a condition of having access to this data, the Local Health Department Participant further agrees to all of the following:

1. The data received can be used for statistical analysis as long as no personally identifiable information is released.

2. The data can be used for public health surveillance, public health program evaluation, and administrative uses. Such uses require a statement of intended use approved by CDPH.

3. Any health research must be approved by the California Health and Human Services Agency's Committee for the Protection of Human Subjects. In addition, any use of confidential birth data for research also requires the approval of the CDPH Vital Statistics Advisory Committee. Data received for health research is deemed confidential and no personally identifiable data are permitted.

4. All data files received must be stored on a secure network consistent with the requirements defined in Section IX. The data must be destroyed when the project described in statement of intended use is completed.

5. Any other release, re-release, or use of birth or death data requires the written permission of the originating state or territory.

VIII. Safeguards: Participant shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of Cal-IVRS 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 IX, Security, below.

IX. Security: The Participant shall take all steps necessary to ensure the continuous security of all of Participant's computerized data systems that access, process, store, receive or transmit Cal-IVRS 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 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 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 Cal-IVRS Data from breaches and security incidents.

C. 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 to this Agreement, which is made a part of this Agreement by this reference.

X. Training: CDPH will provide training to Participant workforce members on the use of Cal-IVRS. The Participant shall provide training on its privacy and security 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 Cal-IVRS 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.

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

XII. 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 XII(G), below. If the breach or security incident occurs after business hours or on a weekend or holiday and involves Cal-IVRS 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 XII(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 Cal-IVRS 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 Cal-IVRS Data and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the Cal-IVRS Data, or to whom it is known (or reasonably believed) to have had the Cal-IVRS Data improperly disclosed to them; and

3. a description of where the Cal-IVRS 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 Cal-IVRS 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 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 XII(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)
Tony Agurto Assistant Deputy Director California Department of Public Health Center for Health Statistics and Informatics 3701 N. Freeway Blvd. P.O. Box 997410, MS 5000 Sacramento, CA 95899-7410 Email: Tony.Agurto@cdph.ca.gov Telephone: (916) 552-8098	**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 1616 Capitol Avenue P.O. Box 997413, MS 6300 Sacramento, CA 95899-7413 Email: cdphiso@cdph.ca.gov Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

XIII. 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 Cal-IVRS Data that was created or collected by Participant in the Cal-IVRS System. Notification shall be provided by CDPH to the Participant Representative, using the contact information listed in Attachment B to this Agreement.

A. 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.

B. 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. Such notice shall be provided to the CDPH Program Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XII(G), above. Said changes shall not require an amendment to this Agreement.

XIV. Indemnification: Participant shall indemnify, hold harmless and defend CDPH 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, its officers, workforce members or agents relative to the Cal-IVRS Data, including without limitation, any violations of Participant's responsibilities under this Agreement.

XV. Term of Agreement: Unless otherwise terminated earlier in accordance with the provisions set forth herein, this Agreement shall remain in effect for five (5) years after the latest signature date in the signature block below. After five (5) 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' advance notice. CDPH may also terminate this Agreement pursuant to Sections XVI or XVII, below.

XVI. Termination for Cause:

A. Termination upon Breach: A breach by Participant 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 Participant 30 days to cure the breach.

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

XVII. 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 Cal-IVRS 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 Cal-IVRS 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 Cal-IVRS Data.

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

XIX. 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 Cal-IVRS Data.

XX. 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.

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 Participant, 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 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.

XXIII. Survival: The respective rights and obligations of Participant under Sections VIII, IX, XII, XIII, and XVIII of this Agreement shall survive the termination or expiration of this Agreement.

XXIV. 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 Cal-IVRS Data; 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.

XXV. 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.

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

XXVII. 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.]

XXVIII. Signatures:

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

On behalf of the Participant, the Nevada County Public Health Department [name of local health department], 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.

Edward Scofield
(Name of Representative of Participant)

Chair, Board of Supervisors
(Title)

(Signature) (Date)

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

(Name of CDPH Representative)

(Title)

(Signature) (Date)

Return Executed Agreement to:

Cal-IVRS
Attention: Support Desk
MS 5103
P.O. Box 997410
Sacramento, CA 95899-7410
FAX: 916-323-2299

Attachment A

Local Health Department Participant

State Law Authority for:

(1) Use and Disclosure of Cal-IVRS Data; and,

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

A. General Legal Authority:

1. California Information Practices Act:

   a. California Civil Code section 1798.24, subdivision (e), provides in part as follows: "No agency may 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: 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…."

B. Specific Legal Authority: Vital Records Collection, Use, and Dissemination

1. Division 102 of the California Health and Safety Code designates that the Director of CDPH is the State Registrar and such duties include the registration, preservation, and dissemination of all of California's birth, death, and marriage records.

2. California Health and Safety Code section 102100 mandates the registration of each live birth, fetal death, death, and marriage that occurs in the state.

3. Division 102 of the California Health and Safety Code designates the health officer of any approved local health department or a person appointed by the State Registrar as the local registrar of birth and deaths which duties include the registration, preservation, dissemination, and transmittal to the State Registrar of the birth and death certificates within that health jurisdiction.

4. Pursuant to California Health and Safety Code section 102405, for live births that occur in a hospital, or a state-licensed alternative birth center, the attending physician and surgeon, certified nurse midwife, or principal attendant, or if the foregoing individuals are unavailable, the administrator of a hospital or center or a representative designated by the administrator in

writing shall be responsible for certifying the live birth and registering the certificate with the local registrar.

5. Pursuant to California Health and Safety Code sections 102780 and 102955, a funeral director, or if there is no funeral director, the person acting in lieu thereof, shall prepare the death or fetal death certificate and register it with the local registrar.

6. California Health and Safety Code section 102230 designates that the State Registrar "shall arrange and permanently preserve the [vital records] certificates in a systematic manner and shall prepare and maintain comprehensive and continuous indices of all certificates registered. Further, California Health and Safety Code section 102230 designates that the State Registrar, at his or her discretion, may release comprehensive birth and death indices to a government agency. A government agency that obtains indices shall not sell or release the index or a portion of its contents to another person except as necessary for official government business and shall not post the indices or any portion thereof on the Internet.

7. Pursuant to California Health and Safety Code section 102430, subdivision (a), the second section of the certificate of live birth as specified in subdivision (b) of California Health and Safety Code section 102425, the electronic file of birth information collected pursuant to subparagraphs (B) to (F), inclusive, of paragraph (2) of subdivision (a) of California Health and Safety Code section 102426, and the second section of the certificate of fetal death as specified in California Health and Safety Code section 103025, are confidential; however, access to this information is authorized for the following: local registrar's staff and local health department staff (when approved by the local registrar or local health officer, respectively), the county coroner, and the birth hospital responsible for preparing and submitting a record of the birth or fetal death for purposes of reviewing and correcting birth or fetal death records.

8. Pursuant to California Health and Safety Code section 103526, subdivision (c)(2)(C), authorized copies of birth and death certificates may be obtained by a representative of another governmental agency, as provided by law, who is conducting official business.

Attachment B

Participant Breach and Security Incident Contact Information.

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

Participant Program Manager	**Participant Privacy Officer**	**Participant Chief Information Security Officer (and IT Service Desk)**
]Name] Patti Carter	]Name] Jeffrey Thorsby	]Name] Steve Monaghan
[Title] Vital Records Supervisor	[Title] Privacy & Security Officer	[Title] Chief Information Oficer
[Address] 500 Crown Point Circle	[Address] 950 Maidu Avenue	[Address] 950 Maidu Avenue
[Address 2]	[Address 2]	[Address 2] 950 Maidu Avenue
[City] Grass Valley	[City] Nevada City	[City] Nevada City
[State, Zip Code] CA 95945	[State, Zip Code] CA 95959	[State, Zip Code] CA 95959
[Telephone] (530) 265-7174	[Telephone] (530) 265-7247	[Telephone] (530) 265-1238
[Fax] (530) 274-8421	[Fax] (530) 265-9836	[Fax] (530) 265-7112
[E-mail] Patti.Carter@co.nevada.ca.us	[E-mail] Jeffrey.Thorsby@co.nevada.ca.us	[E-mail] Steve.Monaghan@co.nevada.ca.us