California Department of Public Health Center for Health Statistics and Informatics

Data Application Agreement

Information Privacy and Security Requirements

This Information Privacy and Security Requirements Agreement (hereinafter referred to as "this Agreement") sets forth the information privacy and security requirements Applicant is obligated to follow with respect to all personal and confidential information (as defined herein) disclosed to Applicant, or collected, created, maintained, stored, transmitted or used by Applicant pursuant to this agreement with the California Department of Public Health (hereinafter "CDPH"). (Such personal and confidential information is referred to herein collectively as "CDPH PCI".) CDPH and Applicant desire to protect the privacy and provide for the security of CDPH PCI pursuant to this Agreement and in compliance with state and federal laws applicable to the CDPH PCI.

I. Order of Precedence: With respect to information privacy and security requirements for all CDPH PCI, the terms and conditions of this Agreement shall take precedence over any conflicting terms or conditions set forth in any other part of the agreement between Applicant and CDPH, including all other Agreements and any other attachments, and shall prevail over any such conflicting terms or conditions.

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 Applicant is obligated to follow with respect to CDPH PCI disclosed to Applicant, or collected, created, maintained, stored, transmitted or used by Applicant for or on behalf of CDPH, pursuant to Applicant's agreement with CDPH. When applicable the Applicant 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 Applicant and CDPH, including this Agreement, the following definitions shall apply:

A. Breach:

"Breach" means:

1. the unauthorized acquisition, access, use, or disclosure of CDPH PCI 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 6252(e), or is exempt from disclosure under any of the provisions of Section 6250, et seq. of the California Government Code or any other applicable

state or federal laws; or

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

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

D. PCI: "PCI" means "personal information" and "confidential information" (as these terms are defined herein:

E. 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.

F. Security Incident: "Security Incident" means:

1. an attempted breach; or

2. the attempted or successful unauthorized access or disclosure, modification, or destruction of CDPH PCI, in violation of any state or federal law or in a manner not permitted under the agreement between Applicant and CDPH, including this Agreement; or

3. the attempted or successful modification or destruction of, or interference with, Applicant's system operations in an information technology system, that negatively impacts the confidentiality, availability, or integrity of CDPH PCI; 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.

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

IV. Disclosure Restrictions: The Applicant and its employees, agents, and subcontractors shall protect from unauthorized disclosure any CDPH PCI. The Applicant shall not disclose, except as otherwise specifically permitted by the agreement between Applicant and CDPH (including this Agreement), any CDPH PCI 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.

V. Use Restrictions: The Applicant and its employees, agents, and subcontractors shall not use any CDPH PCI for any purpose other than performing the Applicant's obligations under its agreement with CDPH.

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

VII. Security: The Applicant shall take any and all steps reasonably necessary to ensure the continuous security of all computerized data systems containing CDPH PCI. These steps shall include, at a minimum, complying with all of the data system security precautions listed in the Applicant Data Security Standards set forth in Attachment 1 to this Agreement.

VIII. Security Officer: At each place where CDPH PCI is located, the Applicant shall designate a Security Officer to oversee its compliance with this Agreement and to communicate with CDPH on matters concerning this Agreement.

IX. Training: The Applicant shall provide training on its obligations under this Agreement, at its

own expense, to all of its employees who assist in the performance of Applicant's obligations under Applicant's agreement with CDPH, including this Agreement, or otherwise use or disclose CDPHPCI.

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

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

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

XI. Breach and Security Incident Responsibilities:

A. Notification to CDPH of Breach or Security Incident: The Applicant shall notify CDPH **immediately by telephone call plus email or fax** upon the discovery of a breach (as defined in this Agreement), **and** within **twenty-four (24) hours by email or fax** 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 CDPH PCI 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 Applicant as of the first day on which such breach or security incident is known to the Applicant, or, by exercising reasonable diligence would have been known to the Applicant. Applicant 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 the Applicant.

Applicant 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: The Applicant shall immediately investigate such breach or security incident. As soon as the information is known and subject to the legitimate needs of law enforcement, Applicant 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 CDPH PCI and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the CDPH PCI, or to whom it is known or reasonably believed to have had the CDPH PCI improperly disclosed to them; and

3. a description of where the CDPH PCI 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: The Applicant 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 Applicant is considered only a custodian and/or non-owner of the CDPH PCI, Applicant 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. Applicant 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 Applicant is considered only a custodian and/or non-owner of the CDPH PCI, Applicant 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). Applicant 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, the Applicant shall initiate contact as indicated herein. CDPH reserves the right to make changes to the contact information below by verbal or written notice to the Applicant. Said changes shall not require an amendment to this Agreement or the agreement to which it is incorporated.

CDPH Program Contract Manager	**CDPH Privacy Officer**	**CDPH Chief Information Security Officer**
See the Data Application Principal Investigator contact information	Privacy Officer Privacy Office, c/o Office of Legal Services California Department of Public Health 1415 L Street, 5th Floor 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 997377 MS6302 Sacramento, CA 95899-7413 Email: cdphiso@cdph.ca.gov Telephone: (855) 500-0016

XII. Documentation of Disclosures for Requests for Accounting: Applicant shall document and make available to CDPH or (at the direction of CDPH) to an Individual such disclosures of

CDPH PCI, 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.

XIII. Requests for CDPH PCI by Third Parties: The Applicant and its employees, agents, or subcontractors shall promptly transmit to the CDPH Program Contract Manager all requests for disclosure of any CDPH PCI requested by third parties to the agreement between Applicant 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.

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

XV. Return or Destruction of CDPH PCI on Expiration or Termination: Upon expiration or termination of the agreement between Applicant and CDPH for any reason, Applicant shall securely return or destroy the CDPH PCI. If return or destruction is not feasible, Applicant shall provide a written explanation 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), above.

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

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

C. Notification of Election to Destroy CDPH PCI: If Applicant elects to destroy the CDPH PCI, Applicant shall certify in writing, 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), above, that the CDPH PCI has been securely destroyed. The notice shall include the date and type of destruction method used.

XVI. Amendment: The parties acknowledge that federal and state laws regarding information security and privacy rapidly evolves 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 CDPH PCI. 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.

XVII. Assistance in Litigation or Administrative Proceedings: Applicant shall make itself and any subcontractors, workforce employees or agents assisting Applicant in the performance of its obligations under the agreement between Applicant 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 the Applicant, except where Applicant or its subcontractor, workforce employee or agent is a named adverse party.

XVIII. 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 Applicant and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

XIX. 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.

XX. Survival: If Applicant does not return or destroy the CDPH PCI upon the completion or termination of the Agreement, the respective rights and obligations of Applicant under Sections VI, VII and XI of this Agreement shall survive the completion or termination of the agreement between Applicant and CDPH.

California Department of Public Health Center for Health Statistics and Informatics

Data Application Agreement

Information Privacy and Security Requirements

Attachment 1
Applicant Data Security Standards

1. General Security Controls

A. ***Confidentiality Statement.*** All persons that will be working with CDPH PCI must sign a confidentiality statement. The statement must include at a minimum, General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to CDPH PCI. The statement must be renewed annually. The Applicant shall retain each person's written confidentiality statement for CDPH inspection for a period of three (3) years following contract termination.

B. ***Background check.*** Before a member of the Applicant's workforce may access CDPH PCI, Applicant must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk for theft of confidential data. The Applicant shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

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

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

E. ***Minimum Necessary.*** Only the minimum necessary amount of CDPH PCI required to perform necessary business functions may be copied, downloaded, or exported.

F. ***Removable media devices.*** All electronic files that contain CDPH PCI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smart devices, backup tapes etc.). PCI must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher

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

H. ***Patch Management.*** All workstations, laptops and other systems that process and/or store CDPH PCI must have operating system and application security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

I. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing CDPH PCI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password.

Passwords are not to be shared. Must be at least eight characters. Must be a non-dictionary word. Must not be stored in readable format on the computer. Must be changed every 60 days. Must be changed if revealed or compromised. Must be composed of characters from at least three of the following four groups from the standard keyboard:

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

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

2. System Security Controls

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

B. ***Warning Banners.*** All systems containing CDPH PCI must display a warning banner each time a user attempts access, stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.

C. ***System Logging*****.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for CDPH PCI, or which alters CDPH PCI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users This logging must be included for all user privilege levels including, but not limited to, systems administrators. If CDPH PCI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

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

E. ***Transmission encryption.*** All data transmissions of CDPH PCI outside the Applicant's secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end-to-end at the network level, or the data files containing CDPH PCI can be encrypted. This requirement pertains to any type of CDPH PCI in motion such as website access, file transfer, and E-Mail.

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

3. Audit Controls

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

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

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

4. Business Continuity / Disaster Recovery Controls

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

B. ***Data Backup Plan.*** Applicant must have established documented procedures to securely backup CDPH PCI to maintain retrievable exact copies of CDPH PCI. The backups shall be encrypted. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore CDPH PCI should it be lost. At a minimum, the schedule must be a

weekly full backup and monthly offsite storage of CDPH data.

5. Paper Document Controls

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

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

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

D. ***Removal of Data.*** CDPH PCI must not be removed from the premises of the Applicant except with express written permission of CDPH.

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

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

I, the undersigned, on behalf of the agency represented in this application, and under penalty of perjury under the laws of the State of California, accept all terms, provisions, and conditions of this application.

Applicant Name *(If the person signing this form is other than the principal investigator or co-principal investigator, please indicate your authority to sign on the organization's behalf):*	
Name of Organization:	

California Department of Public Health Center for Health Statistics and Informatics

Data Application Agreement

Information Privacy and Security Requirements

Organization Address *(physical location where vital records data will be stored and accessed)**:***		
City:	**State:**	**Zip:**
Signature:	**Date:**	