Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

This Information Privacy and Security Requirements Exhibit (For Non-HIPAA/HITECH Act Contracts) (hereinafter referred to as "this Exhibit") sets forth the information privacy and security requirements Contractor is obligated to follow with respect to all personal and confidential information (as defined herein) disclosed to Contractor, or collected ,created, stored, transmitted or used by Contractor for or on **behalf** of the California Department of Public Health (hereinafter "CDPH"), pursuant to Contractor's agreement with CDPH. (Such personal and confidential information is referred to herein collectively as "CDPH PCI".) CDPH and Contractor desire to protect the privacy and provide for the security of CDPH PCI pursuant to this Privacy Exhibit 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 Exhibit shall take precedence over any conflicting terms or conditions set forth in any other part of the agreement between Contractor and CDPH, including Exhibit A (Scope of Work), all other exhibits and any other attachments, and shall prevail over any such conflicting terms or conditions.

II. Affect on lower tier transactions: The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, regardless of whether they are for the acquisition of services, goods, or commodities. When applicable the Contractor shall incorporate the relevant provisions of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

III. Definitions: For purposes of the agreement between Contractor and CDPH, including this Exhibit, the following definitions shall apply:

A. Breach: "Breach" means:

1. the acquisition, access, use, or disclosure of CDPH PCI, in any medium (paper, electronic, oral), in violation of any state or federal law or in a manner not permitted under the agreement between Contractor and CDPH, including this Exhibit, 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(d).

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 he 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; or
3. is "personal information" as defined in this Exhibit.

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

D. Personal Information: "Personal information" means information, in any medium (paper, electronic, oral) that:

1. by itself directly identifies or uniquely describes an individual; or

2. creates a substantial risk that it 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(a) or
4. is one of the data elements set forth in California Civil Code section 1798.29(e)(1),(2) or (3); or
5. meets the definition of "medical information" set forth in either California Civil Code section 1798.29(f)(2) or California Civil Code section 56.05(g); or
6. meets the definition of "health insurance information" set forth in California Civil Code section 1798.29(f)(3).

E. Security Incident: "Security Incident" means:

1. an attempted breach; or
2. the attempted or successful modification or destruction of CDPH PCI, in violation of any state or federal law or in a manner not permitted under the agreement between Contractor and CDPH, (including this Exhibit; or
3. the attempted or successful modification or destruction of, or interference with, Contractor's system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of CDPH PCI, or hinders or makes impossible Contractor's receipt, collection ,creation, storage, transmission or use of PCI by Contractor for or on behalf of CDPH, pursuant to Contractor's agreement with CDPH, including this Exhibit.

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

IV. Disclosure Restrictions: The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure any CDPH PCI. The Contractor shall not disclose, except as otherwise specifically permitted by the agreement between Contractor and CDPH (including this Exhibit) , any CDPH PCI to anyone other than CDPH without prior written authorization from the CDPH Program Contract Manager, except if disclosure is required by State or Federal law.

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

VI. Safeguards: The Contractor 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. The Contractor 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 Contractor's operations and the nature and scope of its activities in performing its agreement with CDPH, including this Exhibit, and which incorporates the requirements of Section VII, Security, below. Contractor shall provide CDPH with Contractor's current and updated policies.

VII. Security: The Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing CDPH PCI. These steps shall include, at a minimum:

A. complying with all of the data system security precautions listed in the Contractor Data Security Standards set forth in Attachment 1 to this Exhibit;
B. 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, which sets forth guidelines for automated information systems in Federal agencies; and

In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to CDPH PCI from breaches and security incidents.

VIII. Security Officer: The Contractor shall designate a Security Officer to oversee its compliance with this Exhibit and for communicating with CDPH on matters concerning this Exhibit.

IX. Training: The Contractor shall provide training on its obligations under this Exhibit, at its own expense, to all of its employees who assist in the performance of Contractor's obligations under Contractor's agreement with CDPH, including this Exhibit, or otherwise use or disclose CDPH PCI.

A. The Contractor shall require each employee who receives training to sign a certification, indicating the employee's name and the date on which the training was completed.
B. The Contractor shall retain each employee's written certifications for CDPH inspection for a period of three years following contract termination.

X. Employee Discipline: Contractor shall discipline such employees and other Contractor workforce members who intentionally violate any provisions of this Exhibit, including by termination of employment.

XI. Breach and Security Incident Responsibilities:

A. Notification to CDPH of Breach or Security Incident: The Contractor shall notify CDPH **immediately by telephone call plus email or fax** upon the discovery of a breach (as defined in this Exhibit), **or** within **twenty-four (24) hours by email or fax** of the discovery of any security incident (as defined in this Exhibit). 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(E), below. If the breach or security incident occurs 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 IIT Service Desk at the telephone numbers listed in Section XI(E), below For purposes of this Section, breaches and security incidents shall be treated as discovered by Contractor as of the first day on which such breach or security incident is known to the Contractor, or, by exercising reasonable diligence would have been known to the Contractor. A Contractor 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 an employee or agent of the Contractor.

Contractor 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: The Contractor shall immediately investigate such breach or security incident, and within seventy-two (72) hours of the discovery, 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 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 believe 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 causes of the breach or security incident; and
5. whether Civil Code sections 1798.29 or any other federal or state laws requiring individual notifications of breaches have been triggered.

C. Written Report: The Contractor 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 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 Contractor is considered only a custodian and/or non-owner of the CDPH PCI, Contractor 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 individuals; or
2. cooperate with and assist CDPH in its notification (including substitute notification) to the individuals affected by the breach.

E. CDPH Contact Information: To direct communications to the above referenced CDPH staff, the Contractor shall initiate contact as indicated herein. CDPH reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Exhibit or the agreement to which it is incorporated.

CDPH Program Contract Manager	**CDPH Privacy Officer**	**CDPH Chief Information Security Officer (and CDPH IT Service Desk)**
See the Scope of Work exhibit for Program Contract Manager	Privacy Officer Privacy Office, c/o Office of Legal Services California Department 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 Department of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413 Email: cdphiso@cdph.ca.gov Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

XII. Documentation of Disclosures for Requests for Accounting: Contractor 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 applicable state or federal law.

XIII. Requests for CDPH PCI by Third Parties: The Contractor and its employees, agents, or subcontractors shall promptly transmit to the CDPH Program Contract Manager all requests for disclosure of any CDPH PCI emanating from third parties to the agreement between Contractor and CDPH (and not emanating from an Individual for an accounting of disclosures of personal information pursuant to applicable state or federal law).

XIV. Audits, Inspection and Enforcement: From time to time, CDPH may inspect the facilities, systems, books and records of Contractor to monitor compliance with this Exhibit. Contractor shall promptly remedy any violation of any provision of this Exhibit and shall certify the same to the CDPH Program Contract Manager in writing. The fact that CDPH inspects, or fails to inspect, or has the right to inspect, Contractor's facilities, systems and procedures does not relieve Contractor of its responsibility to comply with this Exhibit, nor does CDPH's:

A. Failure to detect or

B. Detection, but failure to notify Contractor or require Contractor's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of CDPH's enforcement rights under the agreement and this Exhibit.

XV. Indemnification: Contractor 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 Contractor, its officers, employees, agents or subcontractors relative to the CDPH PCI, including without limitation, any violation ~~s~~ of Contractor's responsibilities under the agreement between it and CDPH, including this Exhibit, with respect to the CDPH PCI.

XVI. Termination:

A. Termination Upon Breach: A breach by Contractor of any provision of the Exhibit, as determined by CDPH, shall constitute a material breach of the agreement between Contractor and CDPH and grounds for immediate termination of the agreement by CDPH. At its sole discretion, CDPH may give Contractor 30 days to cure the breach.

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

XVII. Return or Destruction of CDPH PCI on Expiration or Termination: On expiration or termination of the agreement between Contractor and CDPH for any reason, Contractor shall return or destroy the CDPH PCI. If return or destruction is not feasible, Contractor shall explain to CDPH why, 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(c), above.

A. Retention Required by Law: If Required by state or federal law, Contractor 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: Contractor's obligations under this Exhibit shall continue until Contractor destroys the CDPH PCI or returns the CDPH PCI to CDPH; provided however, that on expiration or termination of the agreement between Contractor and CDPH, Contractor 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: Contractor elects to destroy the CDPH PCI, Contractor 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(c), above. that the CDPH PCI has been destroyed.

XVIII. Amendment: The parties acknowledge that Federal and State laws relating to information security and privacy are rapidly evolving and that amendment of this Exhibit 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. Upon CDPH' request, Contractor agrees to promptly enter into negotiations with CDPH concerning an amendment to this Exhibit 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. Contractor does not promptly enter into negotiations to amend this Exhibit when requested by CDPH pursuant to this Section or
B. Contractor does not enter into an amendment providing assurances regarding the safeguarding of CDPH PCI 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 CDPH PCI.

XIX. Assistance in Litigation or Administrative Proceedings: Contractor shall make itself and any subcontractors, employees or agents assisting Contractor in the performance of its obligations under the agreement between Contractor and CDPH, 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 employees based upon claimed violation of laws relating to security and privacy, which involves inactions or actions by the Contractor, except where Contractor or its subcontractor, employee or agent is a named adverse party.

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

XXI. No Third-Party Beneficiaries: Nothing express or implied in the terms and conditions of this Exhibit is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

XXII. Interpretation: The terms and conditions in this Exhibit 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 Exhibit shall be resolved in favor of a meaning that complies and is consistent with Federal and State regulations.

XXIII. Survival: The respective rights and obligations of Contractor under Sections VI, VII and XI of this Exhibit shall survive the termination or expiration of the agreement between Contractor and CDPH.

Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

Attachment 1
Contractor 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 Contractor 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 Contractor's workforce may access CDPH PCI, Contractor 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 Contractor 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, Blackberry, backup tapes etc.). 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 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 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 PSCI 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 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. 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 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.*** Contractor 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.*** Contractor must have established documented procedures to backup CDPH PCI to maintain retrievable exact copies of CDPH PCI. 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 Contractor 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 CSSI.