Standard Agreement Between County of San Diego and the State of California Department of Public Health
Information Privacy and Security Provisions
Exhibit A – Recitals and Definitions

These Information Privacy and Security Provisions ('Provisions'), including Exhibits A-D, set the requirements County and Contractor are obligated to follow with respect to all personal, sensitive, and confidential information (PSCI), defined herein, disclosed to Contractor, or collected, created, maintained, stored, transmitted, used or disclosed by Contractor for, or on behalf of, the County, pursuant to this Agreement. County and Contractor desire to protect the privacy of and provide for the security of such PSCI pursuant to this Agreement and in compliance with applicable laws.

1. RECITALS

1.1 Order of Precedence: With respect to privacy and security requirements for PSCI, if there is a conflict between any of the requirements contained herein and any other part of the Agreement, then the most stringent shall apply. The most stringent means the requirement which provides the highest level of protection to PSCI.
- 1.1.1 Contractors with access to HIV, Viral Hepatitis, Sexually Transmitted Disease, Tuberculosis, or Ryan White data shall also comply with applicable privacy and security requirements set forth in the Center for Disease Control's 'Data Security and Confidentiality Guidelines.'
- 1.1.2 Contractors of the Ryan White AIDS Drug Assistance Program shall additionally comply with the California Department of Public Health's 'Information Systems Security Requirements for Projects.'

1.2 Effect of lower transactions: The terms of these Provisions shall apply to all contracts, subcontracts, and subawards. Contractor shall enter into written agreements with any Agents that have access to PSCI and otherwise impose the same restrictions and conditions on such Agents that apply to Contractor with respect to such PSCI.

2. DEFINITIONS

2.1 Agents include subcontractors, independent consultants, vendors, and others with whom Contractor contracts to perform work on behalf of County under this Agreement.

2.2 Breach:
- 2.2.1 The unauthorized acquisition, access, use, or disclosure of PSCI, in any medium, in a manner which compromises the security, confidentiality, or integrity of the information or otherwise poses a significant risk of financial, reputational, or other harm to one or more individuals;
- 2.2.2 The same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798;
- 2.2.3 The definition given to such term under HIPAA, defined herein; and/or
- 2.2.4 Is otherwise a violation of applicable law or made impermissible by these Provisions.

2.3 Confidential Information:
- 2.3.1 Information that is not Public Information, defined herein;
- 2.3.2 Meets definition of 'confidential public health record' set forth in California Health and Safety Code 121035; and/or
- 2.3.3 Is contained in documents, files, folders, books, or records clearly labeled, marked, or designated with the word 'confidential' by County or State of California.

2.4 Disclosure:
- 2.4.1 The release, transfer, provision of, access to, or divulging of PSCI, outside the entity holding the PSCI, in any manner; and/or
- 2.4.2 The meaning given to such term under HIPAA.

2.5 Encryption/Encrypted shall mean a Federal Information Processing Standard 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard and should otherwise follow National Institute of Standards and Technology (NIST) 800-111 requirements.

2.6 HIPAA shall encompass the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and the Final Omnibus Rule.

2.7 Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under HIPAA.

2.8 Personal Information shall include:
- 2.8.1 Information in any medium that, by itself, directly or indirectly, collectively identifies or uniquely describes an individual, or 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 other information;
- 2.8.2 The meaning given to such term in California Civil Code 1798;
- 2.8.3 The definition of ‘medical information’ set forth in California Civil Code 1798 and 56.05;
- 2.8.4 The definition of ‘health insurance information’ set forth in California Civil Code 1798; and/or
- 2.8.5 The term ‘Protected Health Information’ as outlined by HIPAA and in these Provisions.

2.9 Personal, Sensitive, and Confidential Information (PSCI), is a term inclusive of each of the three types of information: Personal Information, Sensitive Information, and Confidential Information, defined herein. Contractor should consider all information about individuals served under this Agreement as PSCI, including but not limited to information that County discloses to Contractor or is collected, created, maintained, stored, transmitted, used, or disclosed by Contractor, unless such information is determined to be Public Information, as defined herein.
- 2.9.1 Contractor’s information outside of this Agreement is not considered ‘PSCI’ under these Provisions.

2.10 Protected Health Information (PHI) means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under HIPAA. PHI includes both electronic PHI, as defined by HIPAA, as well as PHI in a non-electronic medium, such as paper or oral PHI.

2.11 Public Information is information that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable laws.

2.12 Security Incidents include:
- 2.12.1 The attempted or actual breach or PSCI;

2.12.2 The attempted or successful unauthorized access, use, disclosure, modification, or destruction of PSCI;
2.12.3 The attempted or successful modification of, destruction of, or interference with Contractor's system operations in an information technology system that negatively impacts confidentiality, availability, or integrity of PSCI;
2.12.4 Any event reasonably believed to have compromised the confidentiality, integrity, or availability of an asset, system, process, data storage, or transmission that contains or provides access to PSCI; and/or
2.12.5 An event that constitutes a violation or imminent threat of violation of Contractor's Information Technology policies and procedures or any portion of these Provisions, including those related to acceptable use.

2.13 Sensitive Information may be either Public Information or Confidential Information. It is information that requires a higher than normal assurance of accuracy and completeness. Sensitive Information may include records of agency financial transactions and regulatory actions.

2.14 Workforce Members shall include employees, interns, volunteers, Agents, and others who have access to PSCI under this Agreement.

This HIPAA Business Associate Agreement Exhibit applies only to those Agreements that involve PHI.

The purpose of this Exhibit is to protect the privacy and security of PHI under this Agreement, and to comply with certain standards and requirements of HIPAA, including, but not limited to, the requirement that County must enter into a contract containing specific requirements with Contractor prior to disclosure of PHI to Contractor, as set forth in HIPAA, as well as the Alcohol and Drug Abuse patient records confidentiality law, 42 CFR Part 2, and other applicable laws.

1. RECITALS

1.1 County wishes to disclose to Contractor certain information pursuant to the terms of the Agreement, some of which may constitute PHI.

1.2 The underlying Agreement, to which this HIPAA Business Associate Agreement Exhibit is attached, has been determined to constitute a business associate relationship under HIPAA.

1.3 Contractor, here and after, is the Business Associate of County, acting on County's behalf.
- 1.3.1 A Contractor's Agent with access to PHI under this Agreement is also a Business Associate.
- 1.3.2 Business Associates are directly liable under HIPAA and subject to civil and/or criminal penalties for making uses or disclosures of PHI that are not authorized by its contracts or required by law and/or for failing to safeguard PHI in accordance with HIPAA.

1.4 Terms in this Exhibit not otherwise defined, shall have the same meanings as defined under HIPAA.

2. RESPONSIBILITIES OF CONTRACTOR

2.1 Uses and Disclosures of PHI
- 2.1.1 Except as otherwise indicated in this Exhibit, Contractor may use or disclose PHI only to perform functions, activities or services specified in the Agreement, provided that such use or disclosure would not violate HIPAA, if done by County. Any such use or disclosure must, to the extent practicable, be limited to the minimum necessary to accomplish the intended purpose of such use or disclosure, and be in compliance with HIPAA and other applicable laws.
  - 2.1.1.1 Contractor may perform data aggregation, meaning the combining of PHI created or received by Contractor on behalf of County with PHI received by Contractor in its capacity as contractor of another covered entity, to permit data analyses that relate to the health care operations of County, with County's express written consent.
- 2.1.2 Contractor shall not:
  - 2.1.2.1 Disclose PHI to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with HIPAA.
  - 2.1.2.2 Directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of County and as permitted by HIPAA.

2.2 Security: Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI, and to protect paper documents containing PHI. These steps shall include, at a minimum:

2.2.1 Achieving and maintaining compliance with HIPAA as necessary in conducting operations on behalf of County under the Agreement; and

2.2.2 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.

2.3 Internal Practices: At County's request, Contractor shall make Contractor's internal practices, books and records relating to PHI available to County or to the Secretary of the U.S. Department of Health and Human Services (DHHS) in a time and manner designated by County or by the Secretary, for purposes of determining County's compliance with HIPAA. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Contractor, Contractor shall so certify to County and shall set forth the efforts it made to obtain the information.

2.4 Audits, Inspections, and Evaluations: If Contractor is the subject of an audit, compliance review, or complaint investigation by the DHHS, which is related to the performance of its obligations pursuant to these Provisions, Contractor shall notify County and provide County with a copy of any information that Contractor provides to DHHS concurrently with providing such information to DHHS. Contractor is responsible for any civil penalties assessed due to an audit or investigation of Contractor, in accordance with 42 U.S.C. section 17934(c) and other applicable laws.

3. OBLIGATIONS OF COUNTY

3.1 Notice of Privacy Practices (NPP): County agrees to provide Contractor with the NPP that County produces in accordance with HIPAA, as well as any changes to such notice. This NPP can be found at www.cosdcompliance.org.

3.2 Permission by Individuals for Use and Disclosure of PHI: County agrees to provide Contractor with any changes in or revocation of, permission by an Individual to use or disclose PHI, if such changes affect Contractor's permitted or required uses and disclosures.

3.3 Notification of Restrictions: County agrees to notify Contractor of any restriction to the use or disclosure of PHI that County has agreed to in accordance with HIPAA, to the extent that such restriction may affect Contractor's use or disclosure of PHI.

3.4 Requests Conflicting with HIPAA Rules: County agrees not to request Contractor to use or disclose PHI in any manner that would not be permissible under HIPAA if done by County.

This "Requirements for Personal, Sensitive, and Confidential Information" (PSCI) Exhibit applies to all contracts which involve PSCI.

1 CONFIDENTIALITY AND SECURITY OF PSCI

1.1 Uses and Disclosures:
- 1.1.1 Contractor shall protect PSCI from unauthorized disclosure.
- 1.1.2 Contractor shall not use or disclose PSCI for any purpose other than carrying out Contractor's obligations under this Agreement.

1.2 Safeguards:
- 1.2.1 Contractor shall implement reasonable and appropriate administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities to protect the privacy, security, confidentiality, integrity, and availability of the PSCI.
- 1.2.2 At each location where PSCI exists, Contractor shall:
  - 1.2.2.1 Develop and maintain a written information privacy and security program that includes reasonable and appropriate administrative, physical, and technical safeguards, including formalized policies and procedures to comply with the requirements herein. Contractor shall provide current and updated policies and procedures related to these safeguards to County within three (3) business days of request by County.
  - 1.2.2.2 Escort visitors in areas where PSCI is contained and keep PSCI out of sight while visitors are in the area.
  - 1.2.2.3 Designate a Security Officer who will oversee and be responsible for carrying out its privacy and security programs and communicate on security matters with County.

2 PERSONNEL CONTROLS

2.1 Employee Training:
- 2.1.1 All Workforce Members who have access to PSCI must complete information privacy and security training covering its obligation under this Agreement, at least annually, at Contractor's expense.
- 2.1.2 Each Workforce Member who receives information privacy and security training must sign a certification, either in hard copy or electronic format, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination. Contractor shall provide copies of certification to County within three (3) business days of request by County.

2.2 Employee Discipline: Appropriate sanctions must be applied against Workforce Members who fail to comply with these Provisions, including termination of employment when appropriate.

2.3 Confidentiality Statement: All Workforce Members with access to PSCI must sign a confidentiality statement that includes, 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 PSCI. The statement must be renewed annually. Contractor shall retain each Workforce Member's written confidentiality statement for County inspection for a period of six (6) years following contract termination.

2.4 Background Check: Before a Workforce Member may access PSCI, a thorough background check of that Workforce Member must be conducted, with evaluation of the results to assure there is no indication that the work force member may present a risk to the security or integrity of PSCI or a risk for theft or misuse of PSCI. Contractor shall retain each Workforce Member's background check documentation for a period of three (3) years following contract termination.

3 TECHNICAL SECURITY CONTROLS

3.1 Workstation/Laptop encryption: All workstations and laptops that process and/or store PSCI must use full disk encryption.

3.2 Server Security: Servers containing unencrypted PSCI must have sufficient administrative, physical, and technical controls in place to protect that PSCI, based upon a risk assessment/system security review.

3.3 Minimum Necessary: Only the minimum necessary PSCI required to perform necessary business functions may be copied, downloaded, or exported and only the minimum necessary Workforce Members given access to PSCI.

3.4 Removable media devices: All electronic files that contain PSCI must be encrypted when stored on any removable media or portable device (i.e. USB drives, smartphones, etc.).

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

3.6 Patch Management: All workstations, laptops and other systems that process and/or store PSCI must have critical 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 thirty (30) calendar days of vendor release.

3.6.1 Contractors on the Syphilis Outbreak program must employ a Patch Management system that meets the following criteria: Vulnerability patching for Common Vulnerability Scoring System (CVSS) "Critical" severity ratings (CVSS 9.0 – 10.0) shall be completed within forty-eight (48) hours of publication or availability of vendor supplied patch: "High" severity rated (CVSS 7.0 – 8.9) shall be completed within seven (7) calendar days of publication or availability of vendor supplied patch: all other vulnerability ratings (CVSS 0.1 – 6.9) shall be completed within thirty (30) days of publication or availability of vendor supplied patch, unless prior approval is granted by the County.

3.7 User IDs and Password Controls:

3.7.1 All Workforce Members who require access to PSCI must be issued a unique username and account ('User Account') for accessing PSCI, which is traceable to an individual.

3.7.2 Each User Account must be promptly disabled upon the transfer or termination of the Workforce Member with knowledge of the password, at maximum within twenty-four (24) hours.

3.7.3 Passwords for User Accounts are not to be shared, nor should system remember user credentials. Passwords must be at least eight characters and must be a non-dictionary word, regardless of language. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
3.7.3.1 Upper case letters (A-Z)
3.7.3.2 Lower case letters (a-z)
3.7.3.3 Arabic numerals (0-9)
3.7.3.4 Non-alphanumeric characters
3.7.4 Passwords for user Accounts must not be stored in readable format on the computer.
3.7.5 Passwords for User Accounts must be changed every ninety (90) calendar days, preferably every sixty (60) days and must be changed immediately if revealed or compromised.
3.7.5.1 If Contractor receives Childhood Lead Poisoning Prevention Program data, Contractor must ensure passwords are changed every sixty (60) days.

3.8 Data Destruction: When no longer needed, all PSCI must be wiped using Gutmann of Department of Defense, DoD 5220.22-M (7 pass), standard or by degaussing. Media may be physically destroyed in accordance with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PSCI cannot be retrieved.

3.9 System Timeout: All systems providing access to PSCI must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

3.10 Warning Banners: All systems providing access to PSCI must display a warning banner stating that data is confidential, system activity is logged, and system use is for business purposes only by authorized users. Workforce members must be directed to log off the system if they do not agree with these requirements.

3.11 System Logging: All systems providing access to PSCI must maintain an automated audit trail which can identify the user or system process which initiates a request for PSCI, or which alters PSCI.
3.11.1 If PSCI is stored in a database, database logging functionality must be enabled.
3.11.2 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.
3.11.3 Logging must be included for all user privilege levels, including but not limited to system administrators.
3.11.4 Audit trail data must be archived for at least three (3) years after occurrence.

3.12 Access Controls: The system providing access to PSCI must use role based access controls for all user authentications, enforcing the principle of least privilege.

3.13 Transmission encryption: All transmissions of PSCI and/or PSCI ‘in motion’ must be encrypted. Encryption can be end-to-end at the network level, or the files containing PSCI can be encrypted.

3.14 Intrusion Detection: All systems involved in accessing, holding, transporting, and protecting PSCI that are accessible via the Internet must install and actively use a real-time, comprehensive intrusion detection and prevention solution.

4 AUDIT CONTROLS

4.1 System Security Review: All systems processing and/or storing PSCI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls, including management, personnel, operations, and IT, are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

4.2 Log Reviews: All systems processing and/or storing PSCI must have a routine procedure to review logs for unauthorized access. Logs and log review documents must be stored for three (3) years.

4.3 Change Control: All systems processing and/or storing PSCI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of PSCI.

5 BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

5.1 Emergency Mode Operation Plan: Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic County PSCI 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 twenty-four (24) hours.

5.2 Data Backup Plan: Contractor must have established documented procedures to securely backup PSCI to maintain retrievable exact copies of PSCI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore PSCI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of PSCI.

6 PAPER AND TRANSPORT CONTROLS

6.1 Supervision of Data: PSCI 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 PSCI is not being observed by a Workforce Member authorized to access the PSCI. PSCI 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.

6.2 Confidential Destruction: Paper PSCI must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization when PSCI is no longer needed, such as crosscut shredding and pulverizing.

6.3 Removal of Data: Paper PSCI must not be removed from the premises of Contractor except with express written permission of County.

6.4 Faxing: Faxes containing PSCI 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 the fax.

6.5 Other Resources: Contractor shall ensure printers, scanners, and other resources used to upload, transmit, or maintain PSCI are located in secure areas.

6.6 Mailing: Mailings of PSCI shall be sealed and secured from damage or inappropriate viewing of PSCI to the extent possible. Mailings which include 500 or more individually identifiable records of PSCI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of County to use another method is obtained. Large volume mailings of PSCI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through mail must be encrypted with a County-approved solution.

7 BREACH AND SECURITY INCIDENT REPORTING The Breach and Security Incident reporting requirements outlined in Article 14 apply to any and all PSCI covered by these Provisions. So too do the definitions of 'breach' and 'security incident' within these Provisions apply to any and all breach and security incident reporting requirements outlined in Article 14.

8 RECORDS

8.1 Access:
- 8.1.1 Contractor shall provide access to PSCI to County, in the time, manner, and medium designated by County (upon reasonable notice and during Contractor's normal business hours).
- 8.1.2 Contractor shall provide access to PSCI, as directed by County, to an Individual, in accordance with applicable law.
- 8.1.3 When applicable, Contractor shall use the forms and processes developed by County for these purposes.
- 8.1.4 Contractor shall promptly transmit to County all requests for disclosure of any PSCI not emanating from the individual or their personal or legal representative.
- 8.1.5 Contractor shall not disclose, except as otherwise specifically permitted by this Agreement to anyone other than County or the State of California without prior written authorization from County, unless disclosure is required by applicable law.

8.2 Accounting of Disclosures:
- 8.2.1 Contractor shall document and make available to County (or at the direction of County to an Individual) such disclosures of PSCI and information related to such disclosures necessary to respond to a proper request by the individual for an accounting of disclosures of personal information as required by applicable law. Contractor shall respond within ten (10) calendar days of receipt of request by County.
- 8.2.2 If Contractor receives PSCI from County that was provided to County by the Social Security Administration, upon request by County, Contractor shall provide County with a list of all Workforce Members who have had access to such PSCI.

8.3 Amendment: Contractor shall make any amendment(s) to PSCI that County directs or agrees to pursuant to applicable law, in the time and manner designated by County.

This “Miscellaneous Terms and Conditions” Exhibit applies to all contracts which involve PSCI. County and Contractor are each a party to this Exhibit and are collectively referred to as the "parties.”

1. AMENDMENT The parties acknowledge that federal and state laws relating to information privacy and security are rapidly evolving and that amendment of these Provisions may be required to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to ensure compliance with such laws.

   1.1 Upon County’s request, Contractor agrees to promptly enter into negotiations with County concerning an amendment to these Provisions, consistent with new standards and requirements imposed by applicable laws.

   1.2 County may terminate this Agreement upon thirty (30) days written notice in the event that Contractor does not promptly enter into negotiations to amend this Agreement.

2. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS Contractor shall make itself and any Workforce Member available to County at no cost to County to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against County, its directors, officers or employees based upon claimed violation of laws related to privacy and security which involves inactions or actions by Contractor, except where Contractor or its Workforce Member is a named adverse party.

3. AUDITS, INSPECTIONS, AND ENFORCEMENT From time to time, County may inspect the facilities, systems, books and records of Contractor to monitor compliance with the Agreement.

   3.1 Contractor shall promptly remedy any violation of any provision of these requirements and, upon County’s request, shall certify the same to County in writing.

   3.2 The fact that County 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 these requirements, nor does County’s failure to detect, or detection, but failure to notify Contractor of requirement to remediate any unsatisfactory practices constitute acceptance of such practices or a waiver of County’ enforcement rights under the Agreement.

4. DISCLAIMER County makes no warranty or representation that Contractor’s compliance Contractor with these Provisions 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 PSCI.

5. DUE DILIGENCE Contractor shall exercise due diligence and shall take reasonable steps to ensure that it and its Workforce Members remain in compliance with these Provisions and are in compliance with applicable law.

6. INDEMNIFICATION Contractor shall indemnify, hold harmless, and defend County and State of California Department of Public Health from and against any and all claims, losses, damages, costs, and other expenses (including attorney's fees) that result from or arise directly/indirectly out of or in connection with any negligent act or omission or willful misconduct of Contractor or its Workforce Members relative to PSCI, including, without limitation, any violations of this Agreement.

7. INTERPRETATION The terms and conditions in these Provisions shall be interpreted as broadly as necessary to implement and comply with HIPAA and other applicable laws. The parties agree that any ambiguity in the terms and conditions of these Provisions shall be resolved in favor of a meaning that complies and is consistent with those laws and regulations.

8. JUDICIAL OR ADMINISTRATIVE PROCEEDINGS Contractor will notify County if it is named as a defendant in a criminal proceeding for a violation of these Provisions. County may terminate the Agreement if Contractor is found guilty of a criminal violation related to this Agreement. County may terminate the Agreement if a finding or stipulation that Contractor has violated any standard or requirement of this Agreement or applicable law is made in any administrative or civil proceeding in which Contractor is a party or has been joined.

9. MITIGATION OF HARMFUL EFFECTS Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PSCI by Contractor or its Workforce Members in violation of the requirements of these Provisions.

10. NO THIRD-PARTY BENEFICIARIES Nothing expressed or implied in the terms and conditions of these Provisions is intended to confer, nor shall anything herein confer, upon any party other than County or Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

11. NO WAIVER OF OBLIGATIONS No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

12. REGULATORY REFERENCES A reference in these Provisions to any privacy or security law or regulation means the section in effect or as amended.

13. RETURN OR DESTRUCTION OF PSCI Upon termination or expiration of the Agreement for any reason, Contractor shall return or destroy all PSCI that Contractor maintains in any form and shall retain no copies of PSCI. If return or destruction is not feasible, Contractor shall provide a written explanation to County and notify County of the conditions that make the return or destruction infeasible, and County and Contractor shall determine the terms and conditions under which Contractor may retain the PSCI.
    13.1 If required by State/federal law, Contractor may retain, after termination of contract, PSCI for time specified to comply with law.
    13.2 Contractor's obligations continue until return or destruction of PSCI

13.2.1 If Contractor elects to destroy PSCI, Contractor shall certify in writing to County that the PSCI has been securely destroyed, as described herein. Notice shall include the date and type of destruction used, as well as a description of the PSCI destroyed.

13.2.2 If return or destruction is infeasible, Contractor shall continue to extend the protections of these Provisions to such PSCI, and shall limit further use of such PSCI to purposes required by applicable law.

14 SURVIVAL The respective rights and obligations of Contractor under these Provisions shall survive the termination or expiration of the Agreement.

15 TERM The Term of these Provisions shall commence as of the effective date of this Agreement, shall extend beyond the termination of the Agreement, and shall terminate when all PSCI is destroyed or returned to County, in accordance with these Provisions and applicable state and federal laws.

16 TERMINATION

16.1 Breach or Violation by County: In accordance with applicable laws, if Contractor knows of a material breach or violation by County of these Provisions, it shall take the following steps:

16.1.1 Provide an opportunity for County to cure the breach or end the violation and terminate the Agreement if County does not cure the breach or end the violation within the time specified by Contractor; or

16.1.2 Immediately terminate the Agreement if County has breached a material term of the Provisions and cure is not possible.

16.2 Breach or Violation by Contractor:

16.2.1 A violation by Contractor of any provision of this Agreement, as determined by County, shall constitute a material ‘breach of contract’ and is grounds for immediate termination of the Agreement by County. At its sole discretion, County may give Contractor up to thirty (30) calendar days to cure the violation.

16.2.2 If Contractor cannot provide assurance regarding safeguarding of PSCI that County in its sole discretion deems sufficient to satisfy the standards/requirements of applicable laws and regulations related to privacy and security of PSCI, and/or contractual requirements imposed on County by the State of California, then County may terminate the Agreement upon thirty (30) calendar days written notice.

16.3 Breach or Violation by Contractor’s Agents: Upon Contractor’s knowledge of a material breach or violation of these Provisions by any of its Agents, Contractor shall:

16.3.1 Provide an opportunity for the Agent to cure the breach or end the violation and terminate the agreement if the Agent does not cure the breach or end the violation within the time specified by County; or

16.3.2 Immediately terminate the agreement if the Agent has breached a material term of these Provisions and cure is not possible.