PROTECTED INFORMATION Privacy and Security Agreement

CONTRACTOR hereby acknowledges and agrees to the following privacy and security obligations and commitments in regard to access to the Department of Public Health's (SFDPH) Protected Information:

a. Compliance with Federal and State Laws. CONTRACTOR shall protect the privacy and provide for the security of SFDPH's medical information or protected health information ("PHI") (collectively, "Protected Information") in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and regulations promulgated there under by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws, including, but not limited to, California Civil Code §§ 56, et seq., California Health and Safety Code § 1280.15, California Civil Code §§ 1798, et seq., California Welfare & Institutions Code §§5328, et seq., and the regulations promulgated there under (the "California Regulations").

b. Attestations. Except when SFDPH's data privacy officer exempts CONTRACTOR in writing, the CONTRACTOR shall complete the following forms, attached and incorporated by reference as though fully set forth herein, SFDPH Attestations for Privacy (Attachment 1), Data Security (Attachment 2), and Compliance (Attachment 3) within sixty (60) calendar days from the execution of the Agreement. If SFDPH makes substantial changes to any of these forms during the term of the Agreement, the CONTRACTOR will be required to complete SFDPH's updated forms within sixty (60) calendar days from the date that SFDPH provides CONTRACTOR with written notice of such changes. CONTRACTOR shall retain such records for a period of seven years after the Agreement terminates and shall make all such records available to SFDPH within 15 calendar days of a written request by SFDPH.

c. Appropriate Safeguards. CONTRACTOR shall take the appropriate security measures to protect the confidentiality, integrity and availability of Protected Information that it accesses, creates, receives, maintains, or transmits.

d. Notification of Breach, Security Threats, and Unpermitted Uses or Disclosures. CONTRACTOR shall notify SFDPH in writing within 5 calendar days of any breach of Protected Information; any reasonable suspicion or detection of security incidents related to Protected Information and any use or disclosure of data in violation of any applicable federal or state laws by CONTRACTOR or its agents or subcontractors. SFDPH will notify CONTRACTOR of any reasonable suspicion or detection of security incidents that could compromise SFDPH systems and confidentiality. In such security incidents, both parties will work collaboratively to mitigate the situation and to identify a solution.

e. Notification of Breach to Regulatory Agencies. CONTRACTOR acknowledges and agrees that, as a Covered Entity and health care provider, it has an obligation independent of SFDPH to notify regulatory agencies and patients of privacy breaches caused by the acts or omissions of its employees or agents or related to the security of its electronic systems.

f. Corrective Action. CONTRACTOR shall take prompt corrective action to remedy any breach of Protected Information, mitigate to the extent practicable any harmful effect of a use or disclosure of Protected Information, and take any other action required by applicable federal and state laws and regulations pertaining to such breach.

g. Protection Against Threats. CONTRACTOR shall protect against any reasonably anticipated threats or hazards to the security or integrity of the Protected Information.

h. Protection Against Unpermitted Uses or Disclosures. CONTRACTOR shall protect against any reasonably anticipated access, uses or disclosures of the Protected Information that are not permitted or required under federal or state law.

i. Security Violations. CONTRACTOR shall maintain written policies and procedures to prevent, detect, contain, and correct security violations, including risk analysis, risk management, sanctions, and information system activity review.

j. Privacy and Security Officers. CONTRACTOR shall maintain qualified Privacy and Security Officers.

k. Appropriate Access. CONTRACTOR shall ensure that all CONTRACTOR employees and agents have appropriate access to electronic Protected Information and shall prevent those employees and agents who do not need access from obtaining it. This includes procedures for authorizing and supervising access, workforce clearance, and personnel termination procedures.

l. Training. CONTRACTOR shall provide privacy and security awareness and training for all employees and agents, including management. This shall include initial training and periodic reminders and updates, including requirements and obligations under federal and state law. Training shall cover protecting against viruses and malicious software and password management.

m. Security Incidents. CONTRACTOR shall maintain policies and procedures to report, mitigate and document Security Incidents.

n. Periodic Evaluations. CONTRACTOR shall conduct periodic evaluations of the security implementation against the Security Standards and environmental or operational changes affecting the security of electronic Protected Information.

o. Facility Access Controls. CONTRACTOR shall maintain facility access controls, which limit physical access to the provider’s electronic information systems and the facilities in which they are housed, while ensuring that authorized access is allowed. These controls include a facility security plan, access control procedures, and facility maintenance.

p. Workstation Use. CONTRACTOR shall maintain security policies and procedures on workstation use, including the physical surroundings of workstations that permit access to electronic Protected Information.

q. Access Controls. CONTRACTOR shall maintain access controls to restrict access to persons or processes that have been granted access rights. These include unique user identification, emergency access procedures, and automatic log off of systems after no more than a ten minute period of inactivity.

r. Audit Control Mechanisms. CONTRACTOR shall comply with SFDPH requests to audit appropriateness of usage of SFDPH electronic records systems. Quarterly, SFDPH shall provide CONTRACTOR with a list representing a random 1% of patient records that were accessed by CONTRACTOR staff during the fiscal year. CONTRACTOR shall develop an audit tool to ensure that the SFDPH electronic records systems are accessed only for treatment reasons, shall conduct quarterly audits, and shall provide the results of these audits to the SFDPH Chief Integrity Officer within 14 calendar days of receipt.

s. Civil and Criminal Penalties. CONTRACTOR understands and agrees that it may be subject to civil or criminal penalties for the unauthorized use, access or disclosure of Protected Information in accordance with the HIPAA Regulations and the HITECH Act including, but not limited to, 42 U.S.C. 17934 (c) and other state and federal laws.

t. Deprovision of Access. Within 24 hours of expiration or earlier termination of the Agreement, CONTRACTOR shall provide SFDPH with a list of all employees and other individuals or entities that have access to SFDPH's electronic records systems. Within 48 hours of expiration or earlier termination of the Agreement, SFDPH shall ensure that all access to SFDPH's electronic records systems is deprovisioned with respect to all individuals and entities on CONTRACTOR's user list.

u. Data Destruction. When no longer needed, CONTRACTOR must destroy all Protected Information received from SFDPH or obtained on SFDPH's behalf that CONTRACTOR has in its possession using the Gutmann or U.S. Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88.

v. Survival. The obligations of CONTRACTOR under this Appendix shall survive the expiration or termination of this Agreement.

w. Disclaimer. SFDPH makes no warranty or representation that compliance by CONTRACTOR with this Agreement, HIPAA, the HITECH Act, the HIPAA Regulations or applicable California law provisions will be adequate or satisfactory for CONTRACTOR's own purposes. CONTRACTOR is solely responsible for all decisions made by CONTRACTOR regarding the safeguarding of PHI.

Attachment 1 – SFDPH Privacy Attestation, version (06-07-17)
Attachment 2 – SFDPH Data Security Attestation, version (06-07-17)
Attachment 3 – SFDPH Compliance Attestation, version (06-07-17)