ATTACHMENT C

ADDITIONAL
REQUIRED PROVISIONS

TABLE OF CONTENTS

1. OVERVIEW 1

2. INFORMATION PRIVACY AND SECURITY 1

2.1 HIPAA OBLIGATIONS 1

2.2 SECURITY REQUIREMENTS 1

2.3 EQUITABLE REMEDIES 1

2.4 PRIVACY AND SECURITY INDEMNIFICATION 2

2.5 SURVIVAL 3

3. INSURANCE REQUIREMENTS 3

4. CONTRACTOR PERSONNEL 3

4.1 MEDICAL HEALTH SCREENING 3

4.2 INFECTION CONTROL 3

5. PROPRIETARY CONSIDERATIONS 4

5.1 INTELLECTUAL PROPERTY 4

5.2 DATA 4

SCHEDULES

SCHEDULE 1 MEDICAL HEALTH SCREENING

SCHEDULE 2 INFORMATION SECURITY AND PRIVACY REQUIREMENTS

SCHEDULE 3 HIPAA COMPLIANCE

SCHEDULE 3.1 BUSINESS ASSOCIATE AGREEMENT

SCHEDULE 4 ADDITIONAL INSURANCE REQUIREMENTS

ADDITIONAL REQUIRED PROVISIONS

1. OVERVIEW

This Attachment C – Additional Required Provisions, including any schedules or other attachments hereto ("Additional Required Provisions"), to the Request for Applications ("RFA") for Miscellaneous Services (RFA No. HASMA-DHS-001) sets forth the terms and conditions for provision of Services pursuant to, and shall become part of and be incorporated into, any Work Order executed as a result of the RFA. These Additional Required Provisions are in addition to the terms and conditions of the Healthcare Ancillary Services Master Agreement ("HASMA") agreed to by the Vendor pursuant to which any Work Order resulting from the RFA shall be executed.

Unless otherwise specified in this Attachment C, those terms with the initial letter capitalized that are not expressly defined herein shall have the meanings given to such terms in the RFA and any executed Work Order(s) as a result of the RFA.

2. INFORMATION PRIVACY AND SECURITY

2.1 HIPAA OBLIGATIONS

Contractor acknowledges that the County is subject the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and regulations promulgated thereunder, including the Privacy, Security, Breach Notification and Enforcement Rules at 45 Code of Federal Regulations ("C.F.R.") Parts 160 and 164 (collectively, "HIPAA Rules"). As a provider of Services for County, Contractor agrees to the applicable provisions relating to HIPAA as specified in Schedule 3 – HIPAA Compliance, attached hereto.

2.2 SECURITY REQUIREMENTS

Contractor's Services and other work provided under the executed Work Order are subject to the requirements specified in this Section 2.2 below, including County's Board Policy No. 5.200 (Contractor Protection of Electronic County Information) as specified below ("Policy"). By executing the Work Order, Contractor (on behalf of itself and any and all employees, agents and subcontractors) certifies its compliance with the Policy and any other requirements specified in this Section 2.2 prior to commencement of Services under the Work Order and for as long as the Contractor (or any of its employees, agents or subcontractors) is in possession of sensitive information (as defined below).

Contractor agrees to comply with the provisions of Schedule 2 (Information Security and Privacy Requirements), including any attachments thereto, on behalf of itself and all persons providing Services pursuant to the executed Work Order.

2.3 EQUITABLE REMEDIES

Failure on the part of Contractor to comply with any of the provisions of this Paragraph 2 shall constitute a material breach of the Master Agreement and the executed Work Order, upon which County may suspend or terminate for default the Master Agreement and/or the executed Work Order, at its sole discretion,

and/or take such other actions as deemed necessary or appropriate by County or required by law. Contractor also acknowledges and agrees that due to the unique nature of the sensitive information addressed in this Paragraph 2 there can be no adequate remedy at law for any breach of Contractor's obligations hereunder, and, therefore, upon any such breach or any threat thereof, County shall be entitled to appropriate equitable remedies and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies County might have at law or equity.

2.4 PRIVACY AND SECURITY INDEMNIFICATION

Notwithstanding any provision of the Master Agreement or the executed Work Order to the contrary, whether expressly or by implication, Contractor shall indemnify, defend and hold harmless County, its officers, employees and agents, from and against any and all claims, demands, damages, liabilities, losses, costs and expenses, including, without limitation, defense costs and legal, accounting and other expert, consulting or professional fees, arising from, connected with or related to any failure by Contractor, including its officers, employees, agents and subcontractors, to comply with the provisions of this Paragraph 2, including but not limited to:

- Contractor's violation of any Federal or State laws in connection with its accessing, collecting, processing, storing, disclosing or otherwise using County Information (as defined in Schedule 2 (Information Security and Privacy Requirements), attached hereto);
- Contractor's failure to perform or comply with any terms or conditions of this Paragraph 2 or Schedule 2 (Information Security and Privacy Requirements), attached hereto; and/or
- Any Information loss, breach of Confidentiality or Incident (as such terms are defined in Schedule 2 (Information Security and Privacy Requirements), attached hereto) involving any County Information that occurs as a result of the fault or negligence of Contractor on Contractor's systems or networks (including all costs and expenses incurred by County to remedy the effects of such loss, breach of Confidentiality or Incident, which may include (i) providing appropriate notice to individuals and governmental authorities, (ii) responding to individuals' and governmental authorities' inquiries, (iii) providing credit monitoring to individuals, and (iv) conducting litigation and settlements with individuals and governmental authorities).

Any legal defense pursuant to Contractor's indemnification obligations under this Paragraph 2 shall be conducted by Contractor and performed by counsel selected by Contractor and approved by County. Notwithstanding the preceding sentence, County shall have the right to participate in any such defense. Contractor shall not have the right to enter into any settlement, agree to any injunction or other equiptable relief, or make any admission, in each case, on behalf of County without County's prior written approval.

2.5 SURVIVAL

The provisions of this Paragraph 2 shall survive the expiration or termination of the Master Agreement and the executed Work Order.

3. INSURANCE REQUIREMENTS

In addition to the insurance requirements specified in the Master Agreement, Contractor shall obtain and maintain for the term of the execued Work Order all insurance programs and coverages as required under Schedule 4 – Additional Insurance Requirements, attached hereto.

4. CONTRACTOR PERSONNEL

4.1 MEDICAL HEALTH SCREENING

Contractor shall ensure that all of Contractor's staff that may provide Services at any County healthcare facility or site (for purposes of this Paragraph, "healthcare campus") pursuant to the executed Work Order, prior to commencement of such Services at a healthcare campus, shall have undergone and successfully passed a current health screening consistent with the DHS policy and the requirements of Schedule 1 – Medical Health Screening, attached hereto ("Medical Health Screening"). The cost of Medical Health Screening shall be borne by Contractor.

4.2 INFECTION CONTROL

4.2.1 Contractor shall ensure that any of Contractor's staff entering any of the County facilities or coming into contact with the public shall comply with and strictly adhere to the applicable County Infection Control and Employee Health Guidelines, provided or made available by County, to prevent the transmission of infections and to ensure prompt and appropriate treatment of Contractor's staff in the event of exposure. If any member of Contractor's staff is diagnosed with having an infectious disease, of which Contractor is made aware, and such person has had contact with a County patient or a member of the public during the usual incubation period for such infectious disease, then the Contractor shall report such occurrence to County's Program Manager, or authorized designee for each site where Services were provided by such staff, within twenty-four (24) hours of becoming aware of the diagnosis. Notwithstanding the foregoing, Contractor shall not allow any member of Contractor's staff to come onto the County premises if Contractor is aware that such person is diagnosed with having an infectious disease.

4.2.2 For purposes of the Master Agreement, the infectious diseases reportable hereunder are those listed in the Public Health List of Reportable Diseases (California Code of Regulations, Title 17).

4.3 BACKGROUND AND SECURITY INVESTIGATIONS

4.3.1 Unless otherwise instructed by County or specified in the Statement of Work, all Contractor personnel providing Services under the Work Order shall undergo and pass, to the satisfaction of County, a background investigation as a condition to beginning and continuing to provide any such

Services. County will use its discretion in determining the method of background clearance to be used, which may include but is not limited to fingerprinting. County may elect to perform the background check.

4.3.2 County may request that Contractor's staff member be immediately prohibited from providing Services under the Work Order at any time during the term of the Work Order, if such staff member does not pass a background investigation to the satisfaction of County or whose background or conduct is incompatible with any Service Site access requirements. County will not provide to Contractor or to Contractor's staff any information obtained through County conducted background clearance.

4.3.3 County may also immediately, at its sole discretion, deny or terminate any Service Site access to Contractor's staff that do not pass such investigation(s) to the satisfaction of County or whose background or conduct is incompatible with such Service Site's access requirements.

4.3.4 Disqualification, if any, of Contractor's staff pursuant to this Paragraph 4.3 shall not relieve Contractor of its obligation to complete all work in accordance with the terms and conditions of the Master Agreement and the Work Order.

5. PROPRIETARY CONSIDERATIONS

5.1 INTELLECTUAL PROPERTY

Contractor hereby grants to County, its authorized users and patients a non-exclusive license to use the Services, including any software and/or equipment utilized for provision of Services and accessed by County or its patients, together with related documentation and other specifications ("License"). Such License shall be in effect at a minimum for the entire duration of the executed Work Order.

5.2 DATA

All data provided by County, including its users and patients, is and shall remain the property of County and is subject to the requirements of Schedule 2 (Information Security and Privacy Requirements), attached hereto, including data destruction and/or return requirements.

SCHEDULE 1
MEDICAL HEALTH SCREENING

All Contractor personnel that may provide services pursuant to the Master Agreement shall complete to the satisfaction of County a medical health screening to determine if the person meets the medical criteria and immunizations standards established for the prospective job classification/assignment before commencing any services under the Master Agreement. Contractor shall use the DHS forms and medical health screening methodology provided or requested by County.

The medical health screening shall be performed by a physician or other licensed healthcare professional ("PLHCP") authorized to perform such screening, with all costs and expenses of such to be borne by Contractor. County, at its sole option, may also elect to have some of the assessments and screening services of Contractor personnel to be provided by DHS Employee Health Services ("EHS"). Upon such election by County, Contractor personnel shall be required to present a written authorization from County prior to obtaining any screening services from DHS EHS. DHS, at its option, will charge Contractor for the costs of any such services provided by DHS EHS or deduct the costs from the amounts owed by County to Contractor for services provided by Contractor under the Master Agreement, regardless of whether Contractor personnel pass or fail the screening.

Each member of Contractor personnel shall provide DHS EHS with documentation of health screenings and evidence of the absence of communicable diseases using the County's "Health Clearance E2" forms. The forms must be signed by a healthcare provider attesting that all information is true and accurate, OR, in the alternative, such member of Contractor personnel may supply all required source documents to DHS EHS for verification.

Contractor must provide DHS EHS with the source documents for each member of Contractor personnel for review within four (4) hours of a request. Failure to provide the appropriate source documentation of health screenings/clearance will result in immediate release of such member of Contractor personnel from assignment without reinstatement until the person is compliant. Contractor shall maintain all source documents pertaining to all Contractor personnel's pre-employment and annual health evaluation, Tuberculosis, Respiratory Fit Testing and other required immunizations including COVID-19 vaccinations.

DHS facility staff are required to ensure that each member of the Contractor personnel (i) receives the appropriate documents; (ii) has submitted them to the applicable DHS facility EHS; and (iii) has obtained health clearance prior to beginning the work assignment under the Master Agreement.

No person shall be allowed to work at any time inside any DHS healthcare providing facility without appropriate documentation of health screening. Lack of evidence of immunity to certain diseases will restrict assignment locations within the DHS facilities.

All Contractor personnel who have potential exposure to respiratory hazards and/or aerosol transmissible disease shall provide appropriate documentation of a respiratory fit test on the same make, model, style and size as the respirator that will be used at the applicable DHS facility. If so instructed by County or the applicable DHS facility, this will be an annual mandatory requirement.

Per County policy, Contractor personnel are required to comply with annual health screening. Unless specified otherwise in the Master Agreement, Contractor personnel shall have their PLHCP conduct the assessment in accordance with County policy and procedures. This

documentation is the “E2 Annual Health Clearance”. Contractor personnel will be provided with the necessary documentation for completion and submission to their PLHCP. The PLHCP will be required to complete the documents and submit them to Contractor, as appropriate, with the completed forms.

Contractor personnel will be given a 30-day reminder to comply with annual health screening requirements. A member of Contractor personnel who does not comply with annual or other health screening requirements may, at County's option, be given a letter indicating that such person has five (5) days to comply or be released from assignment. A copy of the “letter” will be provided to the supervisor/sponsor of such member of Contractor personnel for action. In any event, failure to provide documentation of health screening/clearance will result in immediate release from assignment without reinstatement until compliant.

Contractor personnel potentially exposed to occupational hazards will be provided emergency services within the allowable time frames, with the cost of such emergency services to be borne by Contractor, as appropriate. Contractor personnel who are exposed to occupational hazard or incur injury while performing services for County will be reported on the OSHA Log 300/301, as required by Federal and State regulation and guidelines.

In the event of an occupational needlestick injury or other exposure to Contractor personnel to blood and body fluids or airborne contaminants, medical care will be provided by the DHS EHS or the applicable facility's Emergency Room, with the cost of such medical care to be borne by Contractor, as appropriate. Contractor personnel may seek initial care for such injury or exposure from the facility EHS or DHS EHS within the allowable treatment time frames, with the cost of such care to be borne by Contractor, as appropriate. Subsequent follow-up treatments will be conducted through the appropriate agency’s worker compensation medical provider, or individual’s physician.

SCHEDULE 2
INFORMATION SECURITY AND PRIVACY REQUIREMENTS

CONTRACTOR'S NAME: _____

COUNTY MASTER AGREEMENT / CONTRACT: _____

The County of Los Angeles ("County") is committed to safeguarding the Integrity of County systems, Data, Information and protecting the privacy rights of the individuals that it serves. This Schedule 2 (Information Security and Privacy Requirements (hereinafter referred to as "Exhibit") sets forth County's and Contractor's commitment and agreement to fulfill each of their obligations under applicable state and federal laws, rules and regulations, as well as applicable industry standards concerning privacy, Data protections, Information Security, Confidentiality, Availability and Integrity of such Information. The Information Security and privacy requirements and procedures in this Exhibit are to be established by Contractor before the Effective Date of the Contract (as defined below) and maintained throughout the term of the Contract.

These requirements and procedures are a minimum standard and are in addition to the requirements of the underlying Master Agreement between County and Contractor, including the Work Order executed thereunder (cumulatively, hereinafter "Contract"), and any other agreements between the parties. However, it is Contractor's sole obligation to: (i) implement appropriate and reasonable measures to secure and protect its systems and all County Information against internal and external Threats and Risks; and (ii) continuously review and revise those measures to address ongoing Threats and Risks. Failure to comply with the minimum requirements and procedures set forth in this Exhibit will constitute a material, non-curable breach of Contract by Contractor, entitling County, in addition to the cumulative of all other remedies available to it at law, in equity, or under the Contract, to immediately terminate the Contract. To the extent there are conflicts between this Exhibit and the Contract, this Exhibit shall prevail unless stated otherwise.

1. DEFINITIONS

Unless otherwise defined in the Contract, the definitions herein contained are specific to the uses within this Exhibit.

a. **Availability:** the condition of Information being accessible and usable upon demand by an authorized entity (Workforce Member or process).

b. **Confidentiality:** the condition that Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the Information.

c. **County Information:** all Data and Information belonging to County.

d. **Data:** a subset of Information comprised of qualitative or quantitative values.

e. **Incident:** a suspected, attempted, successful, or imminent Threat of unauthorized electronic and/or physical access, use, disclosure, breach, modification, or destruction of information; interference with Information Technology operations; or significant violation of County policy.

f. **Information:** any communication or representation of knowledge or understanding such as facts, Data, or opinions in any medium or form, including electronic, textual, numerical, graphic, cartographic, narrative, or audiovisual.

g. **Information Security Policy:** high level statements of intention and direction of an organization used to create an organization's Information Security Program as formally expressed by its top management.

h. **Information Security Program:** formalized and implemented Information Security Policies, standards and procedures that are documented describing the program management safeguards and common controls in place or those planned for meeting County's information security requirements.

i. **Information Technology:** any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of Data or Information.

j. **Integrity**: the condition whereby Data or Information has not been improperly modified or destroyed and authenticity of the Data or Information can be ensured.

k. **Mobile Device Management (MDM):** software that allows Information Technology administrators to control, secure, and enforce policies on smartphones, tablets, and other endpoints.

l. **Privacy Policy:** high level statements of intention and direction of an organization used to create an organization's Privacy Program as formally expressed by its top management.

m. **Privacy Program:** A formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the organization's privacy official and other staff, the strategic goals and objectives of the Privacy Program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

n. **Risk:** a measure of the extent to which County is threatened by a potential circumstance or event, Risk is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

o. **Threat:** any circumstance or event with the potential to adversely impact County operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an Information System via unauthorized access, destruction, disclosure, modification of Information, and/or denial of service.

p. **Vulnerability:** a weakness in a system, application, network or process that is subject to exploitation or misuse.

q. **Workforce Member:** employees, volunteers and other persons whose conduct, in the performance of work for County, is under the direct control of County, whether or not they are paid by County. This includes, but may not be limited to, full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to County.

2. INFORMATION SECURITY AND PRIVACY PROGRAMS

a. **Information Security Program.** Contractor shall maintain a company-wide Information Security Program designed to evaluate Risks to the Confidentiality, Availability and Integrity of County Information covered under the Contract.

Contractor's Information Security Program shall include the creation and maintenance

of Information Security Policies, standards, and procedures. Information Security Policies, standards and procedures will be communicated to all Contractor employees in a relevant, accessible and understandable form and will be regularly reviewed and evaluated to ensure operational effectiveness and compliance with all applicable laws and regulations and to address new and emerging Threats and Risks.

Contractor shall exercise the same degree of care in safeguarding and protecting County Information that Contractor exercises with respect to its own Information and Data, but in no event less than a reasonable degree of care. Contractor will implement, maintain and use appropriate administrative, technical and physical security measures to preserve the Confidentiality, Integrity and Availability of County Information.

Contractor's Information Security Program shall:

- Protect the Confidentiality, Integrity and Availability of County Information in Contractor's possession or control;
- Protect against any anticipated Threats or hazards to the Confidentiality, Integrity and Availability of County Information;
- Protect against unauthorized or unlawful access, use, disclosure, alteration and destruction of County Information;
- Protect against accidental loss or destruction of, or damage to, County Information; and
- Safeguard County Information in compliance with any applicable laws and regulations which apply to the Contractor.

b. **Privacy Program.** Contractor shall establish and maintain a company-wide Privacy Program designed to incorporate Privacy Policies and practices in its business operations to provide safeguards for Information, including County Information. Contractor's Privacy Program shall include the development of, and ongoing reviews and updates to Privacy Policies, guidelines, procedures and appropriate workforce privacy training within its organization. These Privacy Policies, guidelines, procedures and appropriate training will be provided to all Contractor employees, agents and volunteers. Contractor's Privacy Policies, guidelines and procedures shall be continuously reviewed and updated for effectiveness and compliance with applicable laws and regulations, and to appropriately respond to new and emerging Threats and Risks. Contractor's Privacy Program shall perform ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

Contractor shall exercise the same degree of care in safeguarding the privacy of County Information that Contractor exercises with respect to its own Information, but in no event less than a reasonable degree of care. Contractor will implement, maintain, and use appropriate privacy practices and protocols to preserve the Confidentiality of County Information.

Contractor's Privacy Program shall include: A Privacy Program framework that identifies and ensures that Contractor complies with all applicable laws and regulations;

- External Privacy Policies, and internal privacy policies, procedures and controls to support the privacy program;
- Protections against unauthorized or unlawful access, use, disclosure, alteration,

or destruction of County Information;

- A training program that covers Privacy Policies, protocols and awareness;
- A response plan to address privacy Incidents and privacy breaches; and
- Ongoing privacy assessments and audits.

3. PROPERTY RIGHTS TO COUNTY INFORMATION

All County Information is deemed property of County, and County shall retain exclusive rights and ownership thereto. County Information shall not be used by Contractor for any purpose other than as required under the Contract, nor shall such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by Contractor, or commercially exploited or otherwise used by, or on behalf of, Contractor, its officers, directors, employees or agents. Contractor may assert no lien on or right to withhold from County, any County Information it receives from, receives addressed to, or stores on behalf of, County. Notwithstanding the foregoing, Contractor may aggregate, compile, and use County Information in order to improve, develop or enhance the System Software and/or other services offered, or to be offered, by Contractor, provided that (i) no County Information in such aggregated or compiled pool is identifiable as originating from, or can be traced back to County, and (ii) such Data or Information cannot be associated or matched with the identity of an individual alone, or linkable to a specific individual. Contractor specifically consents to County's access to such County Information held, stored, or maintained on any and all devices Contactor owns, leases or possesses.

4. CONTRACTOR'S USE OF COUNTY INFORMATION

Contractor may use County Information only as necessary to carry out its obligations under the Contract. Contractor shall collect, maintain, or use County Information only for the purposes specified in the Contract and, in all cases, in compliance with all applicable local, state, and federal laws and regulations governing the collection, maintenance, transmission, dissemination, storage, use, and destruction of County Information, including, but not limited to, (i) any state and federal law governing the protection of personal Information, (ii) any state and federal security breach notification laws, and (iii) the rules, regulations and directives of the Federal Trade Commission, as amended from time to time.

5. SHARING COUNTY INFORMATION AND DATA

Contractor shall not share, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, County Information to a third party for monetary or other valuable consideration.

6. CONFIDENTIALITY

a. **Confidentiality of County Information.** Contractor agrees that all County Information is Confidential and proprietary to County regardless of whether such Information was disclosed intentionally or unintentionally or marked as "confidential".

b. **Disclosure of County Information.** Contractor may disclose County Information only as necessary to carry out its obligations under the Contract, or as required by law, and is prohibited from using County Information for any other purpose without the prior express written approval of County's contract administrator in consultation with County's Chief Information Security Officer and/or Chief Privacy Officer. If required by

a court of competent jurisdiction or an administrative body to disclose County Information, Contractor shall notify County's contract administrator immediately and prior to any such disclosure, to provide County an opportunity to oppose or otherwise respond to such disclosure, unless prohibited by law from doing so.

c. **Disclosure Restrictions of Non-Public Information.** While performing work under the Contract, Contractor may encounter County Non-public Information ("NPI") in the course of performing the Contract, including, but not limited to, licensed technology, drawings, schematics, manuals, sealed court records and other materials described and/or identified as "Internal Use", "Confidential" or "Restricted" as defined in Board of Supervisors Policy 6.104 – Information Classification Policy as NPI. Contractor shall not disclose or publish any County NPI and material received or used in performance of the Contract. This obligation is perpetual.

d. **Individual Requests.** Contractor shall acknowledge any request or instructions from County regarding the exercise of any individual's privacy rights provided under applicable federal or state laws. Contractor shall have in place appropriate policies and procedures to promptly respond to such requests and comply with any request or instructions from County within seven (7) calendar days. If an individual makes a request directly to Contractor involving County Information, Contractor shall notify County within five (5) calendar days and County will coordinate an appropriate response, which may include instructing Contractor to assist in fulfilling the request. Similarly, if Contractor receives a privacy or security complaint from an individual regarding County Information, Contractor shall notify County as described in Section 14 SECURITY AND PRIVACY INCIDENTS, and County will coordinate an appropriate response.

e. **Retention of County Information.** Contractor shall not retain any County Information for any period longer than necessary for Contractor to fulfill its obligations under the Contract and applicable law, whichever is longest.

7. CONTRACTOR EMPLOYEES

Contractor shall perform background and security investigation procedures in the manner prescribed in this Section unless the Contract prescribes procedures for conducting background and security investigations that are no less stringent than the procedures described in this Section.

To the extent permitted by applicable law, Contractor shall screen and conduct background investigations on all Contractor employees and Subcontractors as appropriate to their role for potential security Risks. Such background investigations must be obtained through fingerprints submitted to the California Department of Justice to include State, local and federal level review and conducted in accordance with the law, may include criminal and financial history to the extent permitted under the law and will be repeated on a regular basis. The fees associated with the background investigation shall be borne by Contractor, regardless of whether the member of the Contractor's staff passes or fails the background investigation. Contractor, in compliance with its legal obligations, shall conduct an individualized assessment of their employees, agents, and volunteers regarding the nature and gravity of a criminal offense or conduct; the time that has passed since a criminal offense or conduct and completion of the sentence; and the nature of the access to County Information to ensure that no individual accesses County Information whose past criminal conduct poses a risk or threat to County Information.

Contractor shall require all employees, agents, and volunteers to abide by the requirements in this Exhibit, as set forth in the Contract, and sign an appropriate written Confidentiality/non-disclosure agreement with Contractor.

Contractor shall supply each of its employees with appropriate, annual training regarding Information Security procedures, Risks and Threats. Contractor agrees that training will cover, but may not be limited to the following topics:

a) **Secure Authentication:** The importance of utilizing secure authentication, including proper management of authentication credentials (login name and password) and multi-factor authentication.

b) **Social Engineering Attacks:** Identifying different forms of social engineering including, but not limited to, phishing, phone scams, and impersonation calls.

c) **Handling of County Information:** The proper identification, storage, transfer, archiving and destruction of County Information.

d) **Causes of Unintentional Information Exposure:** Provide awareness of causes of unintentional exposure of Information such as lost mobile devices, emailing Information to inappropriate recipients, etc.

e) **Identifying and Reporting Incidents:** Awareness of the most common indicators of an Incident and how such indicators should be reported within the organization.

f) **Privacy:** Contractor's Privacy Policies and procedures as described in Section 2b. Privacy Program.

Contractor shall have an established set of procedures to ensure Contractor's employees promptly report actual and/or suspected breaches of security.

8. SUBCONTRACTORS AND THIRD PARTIES

County acknowledges that in the course of performing its services, Contractor may desire or require the use of goods, services, and/or assistance of Subcontractors or other third parties or suppliers. The terms of this Exhibit shall also apply to all Subcontractors and third parties. Contractor or third party shall be subject to the following terms and conditions: (i) each Subcontractor and third party must agree in writing to comply with and be bound by the applicable terms and conditions of this Exhibit, both for itself and to enable Contractor to be and remain in compliance with its obligations hereunder, including those provisions relating to Confidentiality, Integrity, Availability, disclosures, security, and such other terms and conditions as may be reasonably necessary to effectuate the Contract including this Exhibit; and (ii) Contractor shall be and remain fully liable for the acts and omissions of each Subcontractor and third party, and fully responsible for the due and proper performance of all Contractor obligations under the Contract.

Contractor shall obtain advance written approval from County's Chief Information Security Officer and/or Chief Privacy Officer, or authorized designee(s), prior to subcontracting any services subject to this Exhibit.

9. STORAGE AND TRANSMISSION OF COUNTY INFORMATION

All County Information shall be rendered unusable, unreadable, or indecipherable to unauthorized individuals. Without limiting the generality of the foregoing, Contractor will encrypt all workstations, portable devices (such as mobile, wearables, tablets,) and removable media (such as portable or removable hard disks, floppy disks, USB memory

drives, CDs, DVDs, magnetic tape, and all other removable storage media) that store County Information in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise approved by County's Chief Information Security Officer.

Contractor shall encrypt County Information transmitted on networks outside of Contractor's control with Transport Layer Security (TLS) 1.2 or higher or Internet Protocol Security (IPSec), at a minimum cipher strength of 128 bit or an equivalent secure transmission protocol or method approved by County's Chief Information Security Officer, or authorized designee.

In addition, Contractor shall not store County Information in the cloud or in any other online storage provider without written authorization from County's Chief Information Security Officer. All mobile devices storing County Information shall be managed by a Mobile Device Management system. Such system must provide provisions to enforce a password/passcode on enrolled mobile devices. All workstations/Personal Computers (including laptops, 2-in-1s, and tablets) will maintain the latest operating system security patches, and the latest virus definitions. Virus scans must be performed at least monthly. Request for less frequent scanning must be approved in writing by County's Chief Information Security Officer.

Furthermore, the hosting environment for storing County Information under the Contract shall be subject to County's approval. Contractor shall also obtain County's approval prior to transitioning data to a different hosting environment by providing, among others, the name of the new hosting environment provider(s), the applicable certifications and the service levels. Contractor warrants and agrees that, notwithstanding County's approval of any changes in the hosting environment, such changes shall not impact Contractor's compliance with the provisions of this Exhibit or performance under the Contract.

10. RETURN OR DESTRUCTION OF COUNTY INFORMATION

Contractor shall return or destroy County Information in the manner prescribed in this Section unless the Contract prescribes procedures for returning or destroying County Information and those procedures are no less stringent than the procedures described in this Section.

a. **Return or Destruction.** Upon County's written request, or upon expiration or termination of the Contract for any reason, Contractor shall (i) promptly return or destroy, at County's option, all originals and copies of all documents and materials it has received containing County Information; or (ii) if return or destruction is not permissible under applicable law, continue to protect such Information in accordance with the terms of the Contract; and (iii) deliver or destroy, at County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by Contractor, prepared under its direction, or at its request, from the documents and materials referred to in Subsection (i) of this Section. For all documents or materials referred to in Subsections (i) and (ii) of this Section that County requests be returned to County, Contractor shall provide a written attestation on company letterhead certifying that all documents and materials have been delivered to County. For documents or materials referred to in Subsections (i) and (ii) of this Section that County requests be destroyed, Contractor shall provide an attestation on company letterhead and certified documentation from a media destruction firm consistent with subdivision b of this Section. Upon termination or expiration of the Contract or at any time upon County's request, Contractor shall

return all hardware, if any, provided by County to Contractor. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by County.

b. **Method of Destruction.** Contractor shall destroy all originals and copies by (i) cross-cut shredding paper, film, or other hard copy media so that the Information cannot be read or otherwise reconstructed; and (ii) purging or destroying electronic media containing County Information consistent with NIST Special Publication 800-88 "Guidelines for Media Sanitization", such that County Information cannot be retrieved. Contractor will provide an attestation on company letterhead and certified documentation from a media destruction firm, detailing the destruction method used and County Information involved, the date of destruction, and the company or individual who performed the destruction. Such statement will be sent to the designated County contract manager within ten (10) days of termination or expiration of the Contract or at any time upon County's request. On termination or expiration of the Contract, County will return or destroy all Contractor's Information marked as confidential (excluding items licensed to County hereunder, or that provided to County by Contractor hereunder), at County's option.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

All Contractor facilities that process County Information must be located in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

All Contractor facilities that process County Information must also be maintained with physical and environmental controls (temperature and humidity) that meet or exceed hardware manufacturer's specifications.

12. OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY AND DISASTER RECOVERY

Contractor shall: (i) monitor and manage all of its Information processing facilities, including, without limitation, implementing operational procedures, change management and Incident response procedures consistent with Section 14 SECURITY AND PRIVACY INCIDENTS; and (ii) deploy adequate anti-malware software and adequate back-up systems to ensure essential business Information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures are adequately documented and designed to protect Information and computer media from theft and unauthorized access.

Contractor shall also maintain and provide business continuity and disaster recovery plans. These plans must include a geographically separate back-up data center and a formal framework by which an unplanned event will be managed to minimize the loss of County Information and services. The formal framework includes a defined back-up policy and associated procedures, including documented policies and procedures designed to: (i) perform back-up of data to a remote back-up data center in a scheduled and timely manner; (ii) provide effective controls to safeguard backed-up data; (iii) securely transfer County Information to and from back- up location; (iv) fully restore applications and operating systems; and (v) demonstrate periodic testing of restoration from back-up location. If Contractor makes backups to removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION), all such backups shall

be encrypted in compliance with the encryption requirements noted above in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

13. ACCESS CONTROL

Subject to and without limiting the requirements under Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION, County Information (i) may only be made available and accessible to those parties explicitly authorized under the Contract or otherwise expressly approved by County's Project Director or County's Project Manager in writing; and (ii) if transferred using removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be sent via a bonded courier and protected using encryption technology designated by Contractor and approved by County's Chief Information Security Officer, or authorized designee, in writing. The foregoing requirements shall apply to back-up media stored by Contractor at off-site facilities.

Contractor shall implement formal procedures to control access to County systems, services, and/or Information, including, but not limited to, user account management procedures and the following controls:

a. Network access to both internal and external networked services shall be controlled, including, but not limited to, the use of industry standard and properly configured firewalls;

b. Operating systems will be used to enforce access controls to computer resources, which shall include without limitation multi-factor authentication, use of virtual private networks (VPN), authorization and event logging;

c. Contractor will conduct regularly, no less frequently than semi-annually, user access reviews to ensure that unnecessary and/or unused access to County Information is removed in a timely manner;

d. Applications will include access control to limit user access to County Information and application system functions;

e. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. Contractor shall record, review and act upon all events in accordance with Incident response policies set forth in Section 14 SECURITY AND PRIVACY INCIDENTS; and

f. In the event any hardware, storage media, or removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be disposed of or sent off-site for servicing, Contractor shall ensure that all County Information, has been eradicated from such hardware and/or media using industry best practices as discussed in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

14. SECURITY AND PRIVACY INCIDENTS

In the event of a Security or Privacy Incident, Contractor shall:

a. Promptly notify the Department of Health Services ("DHS") Chief Information Security Officer, the Departmental Information Security Officer and the DHS Chief Privacy Officer of any Incidents involving County Information, within twenty-four (24) hours of detection of the Incident. All notifications shall be submitted via encrypted email and

telephone to the following:

DHS Chief Information Security Officer and DHS Chief Privacy Officer:

via the Enterprise Help Desk at helpdesk@dhs.lacounty.gov and by phone at (323) 409-8000.

DHS Chief Information Security Officer:

Jeff Zito
jzito@dhs.lacounty.gov

DHS Chief Privacy Officer:

Jennifer Papp, RD, CHPC
jpapp@dhs.lacounty.gov

Departmental Information Security Officer:

Vahe Haratounian
vharatounian@dhs.lacounty.gov

County Chief Information Security Officer and Chief Privacy Officer email

CISO-CPO_Notify@lacounty.gov

b. Include the following Information in all notices:

   i. The date and time of discovery of the Incident,

   ii. The approximate date and time of the Incident,

   iii. A description of the type of County Information involved in the reported Incident, and

   iv. A summary of the relevant facts, including a description of measures being taken to respond to and remediate the Incident, and any planned corrective actions as they are identified.

   v. The name and contact information for the organizations official representative(s), with relevant business and technical information relating to the incident.

c. Cooperate with County to investigate the Incident and seek to identify the specific County Information involved in the Incident upon County's written request, without charge, unless the Incident was caused by the acts or omissions of County. As Information about the Incident is collected or otherwise becomes available to Contractor, and unless prohibited by law, Contractor shall provide Information regarding the nature and consequences of the Incident that are reasonably requested by County to allow County to notify affected individuals, government agencies, and/or credit bureaus.

d. Immediately initiate the appropriate portions of its Business Continuity and/or Disaster Recovery plans in the event of an Incident causing an interference with Information Technology operations.

e. Assist and cooperate with forensic investigators, County, law firms, and and/or law enforcement agencies at the direction of County to help determine the nature, extent and source of any Incident and reasonably assist and cooperate with County on any additional disclosures that County is required to make as a result of the Incident.

f. Allow County or its third-party designee at County's election to perform audits and

tests of Contractor's environment that may include, but are not limited to, interviews of relevant employees, review of documentation or technical inspection of systems, as they relate to the receipt, maintenance, use, retention and authorized destruction of County Information.

Notwithstanding any other provisions in the Contract and Exhibit, Contractor shall be (i) liable for all damages and fines, (ii) responsible for all corrective action, and (iii) responsible for all notifications arising from an Incident involving County Information caused by the Contractor's weaknesses, negligence, errors or lack of Information Security or privacy controls or provisions or otherwise failure to comply with any of the terms or conditions of this Exhibit.

15. NON-EXCLUSIVE EQUITABLE REMEDY

Contractor acknowledges and agrees that due to the unique nature of County Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach may result in irreparable harm to County, and therefore, that upon any such breach, County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies are available within law or equity. Any breach of Section 6 CONFIDENTIALITY shall constitute a material breach of the Contract and be grounds for immediate termination of the Contract in the exclusive discretion of County.

16. AUDIT AND INSPECTION

a. **Self-Audits.** Contractor shall periodically conduct audits, assessments, testing of the system of controls, and testing of Information Security and privacy procedures, including penetration testing, intrusion detection, and firewall configuration reviews. These periodic audits will be conducted by staff certified to perform the specific audit in question at Contractor's sole cost and expense through either (i) an internal independent audit function, (ii) a nationally recognized, external, independent auditor, or (iii) another independent auditor approved by County.

   Contractor shall have a process for correcting control deficiencies that have been identified in the periodic audit, including follow up documentation providing evidence of such corrections. Contractor shall provide the audit results and any corrective action documentation to County promptly upon its completion at County's request. With respect to any other report, certification, or audit or test results prepared or received by Contractor that contains any County Information, Contractor shall promptly provide County with copies of the same upon County's reasonable request, including identification of any failure or exception in Contractor's Information systems, products, and services, and the corresponding steps taken by Contractor to mitigate such failure or exception. Any reports and related materials provided to County pursuant to this Section shall be provided at no additional charge to County.

b. **County Requested Audits.** At its own expense, County or an independent third-party auditor commissioned by County shall have the right to audit Contractor's infrastructure, security and privacy practices, Data center, services and/or systems storing or processing County Information via an onsite inspection at least once a year. Upon County's request Contractor shall complete a questionnaire regarding Contractor's Information Security and/or program. County shall pay for County requested audit unless the auditor finds that Contractor has materially breached this

Exhibit, in which case Contractor shall bear all costs of the audit**;** and if the audit reveals material non-compliance with this Exhibit, County may exercise its termination rights underneath the Contract.

Such audit shall be conducted during Contractor's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect Contractor's normal business operations. County's request for the audit will specify the scope and areas (e.g., Administrative, Physical, and Technical) that are subject to the audit and may include, but are not limited to physical controls inspection, process reviews, policy reviews, evidence of external and internal Vulnerability scans, penetration test results, evidence of code reviews, and evidence of system configuration and audit log reviews. It is understood that the results may be filtered to remove the specific Information of other Contractor customers such as IP address, server names, etc. Contractor shall cooperate with County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. This right of access shall extend to any regulators with oversight of County. Contractor agrees to comply, within acceptable reasonable timeframes, with all reasonable recommendations that result from such inspections, tests and audits.

When not prohibited by regulation, Contractor will provide to County a summary of: (i) the results of any security audits, security reviews, or other relevant audits, conducted by Contractor or a third party; and (ii) corrective actions or modifications, if any, Contractor will implement in response to such audits.

17. CYBER LIABILITY INSURANCE

Contractor shall secure and maintain cyber liability insurance coverage in the manner prescribed in this Section unless the Contract prescribes cyber liability insurance coverage provisions and those provisions are no less stringent than those described in this Section.

Contractor shall secure and maintain cyber liability insurance coverage with limits of at least $10,000,000 per occurrence and in the aggregate during the term of the Contract, including coverage for: network security liability; privacy liability; privacy regulatory proceeding defense, response, expenses and fines; technology professional liability (errors and omissions); privacy breach expense reimbursement (liability arising from the loss or disclosure of County Information no matter how it occurs); system breach; denial or loss of service; introduction, implantation, or spread of malicious software code; unauthorized access to or use of computer systems; and Data/Information loss and business interruption; any other liability or risk that arises out of Contract. Contractor shall add County as an additional insured to its cyber liability insurance policy and provide to County certificates of insurance evidencing the foregoing upon County's request. The procuring of the insurance described herein, or delivery of the certificates of insurance described herein, shall not be construed as a limitation upon Contractor's liability or as full performance of its indemnification obligations hereunder. No exclusion/restriction for unencrypted portable devices/media may be on the policy.

18. PRIVACY AND SECURITY INDEMNIFICATION

In addition to the indemnification provisions in the Contract, Contractor agrees to indemnify, defend, and hold harmless County, its Special Districts, elected and appointed officers, agents, employees, and volunteers from and against any and all claims,

demands liabilities, damages, judgments, awards, losses, costs, expenses or fees including reasonable attorneys' fees, accounting and other expert, consulting or professional fees, and amounts paid in any settlement arising from, connected with, or relating to :

- Contractor's violation of any federal and state laws in connection with its accessing, collecting, processing, storing, disclosing or otherwise using County Information;
- Contractor's failure to perform or comply with any terms and conditions of the Contract or related agreements with County; and/or
- Any Information loss, breach of Confidentiality, or Incident involving any County Information that occurs on the Contractor's systems or networks (including all costs and expenses incurred by County to remedy the effects of such loss, breach of Confidentiality, or Incident, which may include (i) providing appropriate notice to individuals and governmental authorities, (ii) responding to individuals' and governmental authorities' inquiries, (iii) providing credit monitoring to individuals, and (iv) conducting litigation and settlements with individuals and governmental authorities). Notwithstanding the preceding sentences, County shall have the right to participate in any such defense at its sole cost and expense, except that in the event contractor fails to provide County with a full and adequate defense, as determined by County in its sole judgment, County shall be entitled to retain its own counsel, including, without limitation, County Counsel, and to reimbursement from contractor for all such costs and expenses incurred by County in doing so. Contractor shall not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of County without County's prior written approval.

ADDENDUM A: SOFTWARE AS A SERVICE (SaaS)

a. **License:** Subject to the terms and conditions set forth in the Contract, including payment of the license fees by to Contractor, Contractor hereby grants to County a non-exclusive, non-transferable worldwide County license to use the SaaS, as well as any documentation and training materials, during the term of the Contract to enable County to use the full benefits of the SaaS and achieve the purposes stated herein.

b. **Business Continuity:** In the event that Contractor's infrastructure containing or processing County Information becomes lost, altered, damaged, interrupted, destroyed or otherwise limited in functionality in a way that affects County's use of the SaaS, Contractor shall immediately and within twenty two (2) hours implement Contractor's Business Continuity Plan, consistent with Section 12 OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY, such that Contractor can continue to provide full functionality of the SaaS as described in the Contract.

   Contractor will indemnify County for any claims, losses, or damages arising out of County's inability to use the SaaS consistent with the Contract and Section 18 PRIVACY AND SECURITY INDEMNIFICATION.

   Contractor shall include in its Business Continuity Plan service offering, a means for segmenting and distributing IT infrastructure, disaster recovery and mirrored critical system, among any other measures reasonably necessary to ensure business continuity and provision of the SaaS.

   In the event that the SaaS is interrupted, County Information may be accessed and retrieved within two (24) hours at any point in time. To the extent Contractor hosts County Information related to the SaaS, Contractor shall create daily backups of all County Information related to County's use of the SaaS in a segmented or off-site "hardened" environment in a manner that ensures backups are secure consistent with cybersecurity requirements described in the Contract and available when needed.

c. **Enhancements:** Upgrades, replacements and new versions: Contractor agrees to provide to County, at no cost, prior to, and during installation and implementation of the SaaS any software/firmware enhancements, upgrades, and replacements which Contractor initiates or generates that are within the scope of the SaaS and that are made available at no charge to the Contractor's other customers.

   During the term of the Contract, Contractor shall promptly notify County of any available updates, enhancements or newer versions of the SaaS and within thirty (30) Days update or provide the new version to County. Contractor shall provide any accompanying documentation in the form of new or revised documentation necessary to enable County to understand and use the enhanced, updated, or replaced SaaS.

   During the Contract term, Contractor shall not delete or disable a feature or functionality of the SaaS unless Contractor provides sixty (60) Days advance notice and County provides written consent to delete or disable the feature or functionality. Should there be a replacement feature or functionality, County shall have the sole discretion whether to accept such replacement. The replacement shall be at no additional cost to County. If Contractor fails to abide by the obligations in this Section, County reserves the right to terminate the Contract for material breach and receive a pro-rated refund.

d. **Location of County Information:** Contractor warrants and represents that it shall store and process County Information only in the continental United States and that at no time will County Data traverse the borders of the continental United States in an unencrypted manner.

e. **Audit and Certification:** Contractor agrees to conduct an annual System and Organization Controls (SOC 2 type II) audit or equivalent (i.e. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001:2013 certification audit or Health Information Trust Alliance (HITRUST) Common Security Framework certification audit) of its internal controls for security, availability, integrity, confidentiality, and privacy. Contractor shall have a process for correcting control deficiencies that have been identified in the audit, including follow up documentation providing evidence of such corrections. The results of the audit and Contractor's plan for addressing or resolving the audit findings shall be shared with County's Chief Information Security Officer within ten (10) business days of the Contractor's receipt of the audit results. Contractor agrees to provide County with the current audit certifications upon request.

f. **Services Provided by a Subcontractor:** Prior to the use of any Subcontractor for the SaaS under the Contract, Contractor shall notify County of the proposed subcontractor(s) and the purposes for which they may be engaged at least thirty (30) Days prior to engaging the Subcontractor and obtain written consent of County's Contract Administrator.

g. **Information Import Requirements at Termination:** Within one (1) Day of notification of termination of the Contract, Contractor shall provide County with a complete, portable, and secure copy of all County Information, including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in a format to be determined by County upon termination.

h. **Termination Assistance Services:** During the ninety (90) Day period prior to, and/or following the expiration or termination of the Contract, in whole or in part, Contractor agrees to provide reasonable termination assistance services at no additional cost to County, which may include:

   i. Developing a plan for the orderly transition of the terminated or expired SaaS from Contractor to a successor;

   ii. Providing reasonable training to County staff or a successor in the provision of the SaaS currently being provided by Contractor;

   iii. Using its best efforts to assist and make available to County any third-party services then being used by Contractor in connection with the SaaS; and

   iv. Such other activities upon which the parties may reasonably agree.

   The termination assistance services shall be provided at no cost to County, unless otherwise agreed to by the parties.

SCHEDULE 3
HIPAA COMPLIANCE

SCHEDULE 3.1
BUSINESS ASSOCIATE AGREEMENT

County is a Covered Entity as defined by, and subject to the requirements and prohibitions of, the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (hereinafter “HIPAA”) and regulations promulgated thereunder, including the Privacy, Security, Breach Notification and Enforcement Rules at 45 Code of Federal Regulations (hereinafter “C.F.R.”) Parts 160 and 164 (hereinafter collectively, “HIPAA Rules”).

Contractor performs or provides functions, activities, services or other work (hereinafter "Services") to County that require Contractor in order to provide such Services to create, access, receive, maintain and/or transmit information that includes or that may include Protected Health Information, as defined by the HIPAA Rules. As such, Contractor is a Business Associate, as defined by the HIPAA Rules, and is therefore subject to those provisions of the HIPAA Rules that are applicable to Business Associates.

The HIPAA Rules require a written agreement (hereinafter "Business Associate Agreement") between County and Contractor in order to mandate certain protections for the privacy and security of Protected Health Information, and these HIPAA Rules prohibit the disclosure to or use of Protected Health Information by Contractor if such an agreement is not in place.

This Business Associate Agreement and its provisions are intended to protect the privacy and provide for the security of Protected Health Information disclosed to or used by Contractor in compliance with the HIPAA Rules.

Therefore, the parties agree as follows:

1. DEFINITIONS

1.1 "Breach" has the same meaning as the term "breach" at 45 C.F.R. § 164.402.

1.2 "Business Associate" has the same meaning as the term "business associate" at 45 C.F.R. § 160.103. For the convenience of the parties, a "business associate" is a person or entity, other than a member of the workforce of covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to Protected Health Information. A "business associate" also is a subcontractor that creates, receives, maintains or transmits Protected Health Information on behalf of another business associate. And in reference to the party to this Business Associate Agreement "Business Associate" shall mean Contractor.

1.3 "Covered Entity" has the same meaning as the term “covered entity” at 45 C.F.R. § 160.103, and, in reference to the party to this Business Associate Agreement, "Covered Entity" shall mean County.

1.4 "Data Aggregation" has the same meaning as the term "data aggregation" at 45 C.F.R. § 164.501.

1.5 "De-identification" refers to the de-identification standard at 45 C.F.R. § 164.514.

1.6 "Designated Record Set" has the same meaning as the term "designated record set" at 45 C.F.R. § 164.501.

1.7 "Disclose" and "Disclosure" mean, with respect to Protected Health Information, the release, transfer, provision of access to, or divulging in any other manner of Protected Health Information outside Business Associate's internal operations or to other than its workforce. (See 45 C.F.R. § 160.103.)

1.8 "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff. (See 42 U.S. C. § 17921.)

1.9 "Electronic Media" has the same meaning as the term "electronic media" at 45 C.F.R. § 160.103. For the convenience of the parties, electronic media means (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

1.10 "Electronic Protected Health Information" has the same meaning as the term "electronic protected health information" at 45 C.F.R. § 160.103, limited to Protected Health Information created or received by Business Associate from or on behalf of Covered Entity. For the convenience of the parties, the term "Electronic Protected Health Information" means Protected Health Information that is (i) transmitted by electronic media; (ii) maintained in electronic media.

1.11 "Health Care Operations" has the same meaning as the term "health care operations" at 45 C.F.R. § 164.501.

1.12 "Individual" has the same meaning as the term "individual" at 45 C.F.R. § 160.103. For the convenience of the parties, Individual means the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502 (g).

1.13 "Law Enforcement Official" has the same meaning as the term "law enforcement official" at 45 C.F.R. § 164.103.

1.14 "Minimum Necessary" refers to the minimum necessary standard at 45 C.F.R. § 164.502(b).

1.15 "Protected Health Information" has the same meaning as the term "protected health information" at 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity. For the convenience of the parties, Protected Health Information includes information that (i) 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; (ii) identifies the Individual (or for which there is a reasonable basis for believing that the information can be used to identify the Individual); and (iii) is created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity, and includes Protected Health Information that is made accessible to Business Associate by Covered Entity. "Protected Health Information" includes Electronic Protected Health Information.

1.16 "Required by Law" " has the same meaning as the term "required by law" at 45 C.F.R. § 164.103.

1.17 "Secretary" has the same meaning as the term "secretary" at 45 C.F.R. § 160.103

1.18 "Security Incident" has the same meaning as the term "security incident" at 45 C.F.R. § 164.304.

1.19 "Services" means, unless otherwise specified, those functions, activities, services or other work in the applicable underlying Agreement, Contract, Master Agreement, Work Order, or Purchase Order or other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

1.20 "Subcontractor" has the same meaning as the term "subcontractor" at 45 C.F.R. § 160.103.

1.21 "Unsecured Protected Health Information" has the same meaning as the term "unsecured protected health information" at 45 C.F.R. § 164.402.

1.22 "Use" or "Uses" means, with respect to Protected Health Information, the sharing, employment, application, utilization, examination or analysis of such Information within Business Associate's internal operations. (See 45 C.F.R § 164.103.)

1.23 Terms used, but not otherwise defined in this Business Associate Agreement, have the same meaning as those terms in the HIPAA Rules.

2. PERMITTED AND REQUIRED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

2.1 Business Associate may only Use and/or Disclose Protected Health Information as necessary to perform Services and/or as necessary to comply with the obligations of this Business Associate Agreement.

2.2 Business Associate may Use Protected Health Information for de-identification of the information if de-identification of the information is required to provide Services.

2.3 Business Associate may Use or Disclose Protected Health Information as Required by Law.

2.4 Business Associate shall make Uses and Disclosures and requests for Protected Health Information consistent with the Covered Entity's applicable Minimum Necessary policies and procedures.

2.5 Business Associate may Use Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities.

2.6 Business Associate may Disclose Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities, provided the Disclosure is Required by Law or Business Associate obtains reasonable assurances from the person to whom the Protected Health Information is disclosed (i.e., the recipient) that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purposes for which it was disclosed to the recipient and the recipient notifies Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached.

2.7 Business Associate may provide Data Aggregation services relating to Covered Entity's Health Care Operations if such Data Aggregation services are necessary in order to provide Services.

3. PROHIBITED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

3.1 Business Associate shall not Use or Disclose Protected Health Information other than as permitted or required by this Business Associate Agreement or as Required by Law.

3.2 Business Associate shall not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except for the specific Uses and Disclosures set forth in Sections 2.5 and 2.6.

3.3 Business Associate shall not Use or Disclose Protected Health Information for de-identification of the information except as set forth in Section 2.2.

4. OBLIGATIONS TO SAFEGUARD PROTECTED HEALTH INFORMATION

4.1 Business Associate shall implement, use, and maintain appropriate safeguards to prevent the Use or Disclosure of Protected Health Information other than as provided for by this Business Associate Agreement.

4.2 Business Associate shall comply with Subpart C of 45 C.F.R Part 164 with respect to Electronic Protected Health Information to prevent the Use or Disclosure of such information other than as provided for by this Business Associate Agreement.

5. REPORTING NON-PERMITTED USES OR DISCLOSURES, SECURITY INCIDENTS AND BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION

5.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information not permitted by this Business Associate Agreement, any Security Incident and/ or any Breach of Unsecured Protected Health Information, as further described in Sections 5.1.1, 5.1.2 and 5.1.3.

5.1.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information by Business Associate, its employees, representatives, agents or Subcontractors not provided for by the Agreement of which Business Associate becomes aware.

5.1.2 Business Associate shall report to Covered Entity any Security Incident of which Business Associate becomes aware.

5.1.3 Business Associate shall report to Covered Entity any Breach by Business Associate, its employees, representatives, agents, workforce members or Subcontractors of Unsecured Protected Health Information that is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate. Business Associate shall be deemed to have knowledge of a Breach of Unsecured Protected Health Information if the 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, officer or other agent of Business Associate, including a Subcontractor, as determined in accordance with the Federal common law of agency.

5.2 Except as provided in Section 5.3, for any reporting required by Section 5.1, Business Associate shall provide, to the extent available, all information required by, and within the times frames specified in, Sections 5.2.1 and 5.2.2.

5.2.1 Business Associate shall make an immediate telephonic report upon discovery of the non-permitted Use or Disclosure of Protected Health Information, Security Incident or Breach of Unsecured Protected Health Information to **(562) 940-3335** that minimally includes:

(a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident or Breach, if known;

(b) The number of Individuals whose Protected Health Information is involved;

(c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(d) The name and contact information for a person highly knowledgeable of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident or Breach.

5.2.2 Business Associate shall make a written report without unreasonable delay and in no event later than three (3) business days from the date of discovery by Business Associate of the non-permitted Use or Disclosure of Protected Health Information, Security Incident or Breach of Unsecured Protected Health Information to the **HIPAA Compliance Officer at: Hall of Records, County of Los Angeles, Chief Executive Office, Risk Management Branch-Office of Privacy, 320 W. Temple Street, 7th Floor, Los Angeles, California 90012, PRIVACY@ceo.lacounty.gov** that includes, to the extent possible:

(a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident or Breach, if known;

(b) The number of Individuals whose Protected Health Information is involved;

(c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(d) The identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, Used or Disclosed;

(e) Any other information necessary to conduct an assessment of whether notification to the Individual(s) under 45 C.F.R. § 164.404 is required;

(f) Any steps Business Associate believes that the Individual(s) could take to protect him or herself from potential harm from the non-permitted Use or Disclosure, Security Incident or Breach;

(g) A brief description of what Business Associate is doing to investigate, to mitigate harm to the Individual(s) and to protect against any further similar occurrences; and

(h) The name and contact information for a person highly knowledgeable of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident or Breach.

5.2.3 If Business Associate is not able to provide the information specified in Section 5.2.1 or 5.2.2 at the time of the required report, Business Associate shall provide such information promptly thereafter as such information becomes available.

5.3 Business Associate may delay the notification required by Section 5.1.3, if a law enforcement official states to Business Associate that notification would impede a criminal investigation or cause damage to national security.

5.3.1 If the law enforcement official's statement is in writing and specifies the time for which a delay is required, Business Associate shall delay its reporting and/or notification obligation(s) for the time period specified by the official.

5.3.2 If the statement is made orally, Business Associate shall document the statement, including the identity of the official making the statement and delay its reporting and/or notification obligation(s) temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in Section 5.3.1 is submitted during that time.

6. WRITTEN ASSURANCES OF SUBCONTRACTORS

6.1 In accordance with 45 C.F.R. § 164.502 (e)(1)(ii) and § 164.308 (b)(2), if applicable, Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of Business Associate is made aware of its status as a Business Associate with respect to such information and that Subcontractor agrees in writing to the same restrictions, conditions and requirements that apply to Business Associate with respect to such information.

6.2 Business Associate shall take reasonable steps to cure any material breach or violation by Subcontractor of the agreement required by Section 6.1.

6.3 If the steps required by Section 6.2 do not cure the breach or end the violation, Contractor shall terminate, if feasible, any arrangement with Subcontractor by which Subcontractor creates, receives, maintains or transmits Protected Health Information on behalf of Business Associate.

6.4 If neither cure nor termination as set forth in Sections 6.2 and 6.3 is feasible, Business Associate shall immediately notify County.

6.5 Without limiting the requirements of Section 6.1, the agreement required by Section 6.1 (Subcontractor Business Associate Agreement) shall require Subcontractor to contemporaneously notify Covered Entity in the event of a Breach of Unsecured Protected Health Information.

6.6 Without limiting the requirements of Section 6.1, agreement required by Section 6.1 (Subcontractor Business Associate Agreement) shall include a provision requiring Subcontractor to destroy or, in the alternative to return to Business Associate, any Protected Health Information created, received, maintained or transmitted by Subcontractor on behalf of Business Associate so as to enable Business Associate to comply with the provisions of Section 18.4.

6.7 Business Associate shall provide to Covered Entity, at Covered Entity's request, a copy of any and all Subcontractor Business Associate Agreements required by Section 6.1.

6.8 Sections 6.1 and 6.7 are not intended by the parties to limit in any way the scope of Business Associate's obligations related to Subcontracts or Subcontracting in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

7. ACCESS TO PROTECTED HEALTH INFORMATION

7.1 To the extent Covered Entity determines that Protected Health Information is maintained by Business Associate or its agents or Subcontractors in a Designated Record Set, Business Associate shall, within two (2) business days after receipt of a request from Covered Entity, make the Protected Health Information specified by Covered Entity available to the Individual(s) identified by Covered Entity as being entitled to access and shall provide such Individuals(s) or other person(s) designated by Covered Entity with a copy the specified Protected Health Information, in order for Covered Entity to meet the requirements of 45 C.F.R. § 164.524.

7.2 If any Individual requests access to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within two (2) days of the receipt of the request. Whether access shall be provided or denied shall be determined by Covered Entity.

7.3 To the extent that Business Associate maintains Protected Health Information that is subject to access as set forth above in one or more Designated Record Sets electronically and if the Individual requests an electronic copy of such information, Business Associate shall provide the Individual with access to the Protected Health Information in the electronic form and format requested by the Individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by Covered Entity and the Individual.

8. AMENDMENT OF PROTECTED HEALTH INFORMATION

8.1 To the extent Covered Entity determines that any Protected Health Information is maintained by Business Associate or its agents or Subcontractors in a Designated Record Set, Business Associate shall, within ten (10) business days after receipt of a written request from Covered Entity, make any amendments to such Protected Health Information that are requested by Covered Entity, in order for Covered Entity to meet the requirements of 45 C.F.R. § 164.526.

8.2 If any Individual requests an amendment to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the receipt of the request. Whether an amendment shall be granted or denied shall be determined by Covered Entity.

9. ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

9.1 Business Associate shall maintain an accounting of each Disclosure of Protected Health Information made by Business Associate or its employees, agents, representatives or Subcontractors, as is determined by Covered Entity to be necessary in order to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

9.1.1 Any accounting of disclosures provided by Business Associate under Section 9.1 shall include:

(a) The date of the Disclosure;

(b) The name, and address if known, of the entity or person who received the Protected Health Information;

(c) A brief description of the Protected Health Information Disclosed; and

(d) A brief statement of the purpose of the Disclosure.

9.1.2 For each Disclosure that could require an accounting under Section 9.1, Business Associate shall document the information specified in Section 9.1.1 and shall maintain the information for six (6) years from the date of the Disclosure.

9.2 Business Associate shall provide to Covered Entity, within ten (10) business days after receipt of a written request from Covered Entity, information collected in accordance with Section 9.1.1 to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

9.3 If any Individual requests an accounting of disclosures directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the receipt of the request and shall provide the requested accounting of disclosures to the Individual(s) within 30 days. The information provided in the accounting shall be in accordance with 45 C.F.R. § 164.528.

10. COMPLIANCE WITH APPLICABLE HIPAA RULES

10.1 To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity's performance of such obligation(s).

10.2 Business Associate shall comply with all HIPAA Rules applicable to Business Associate in the performance of Services.

11. AVAILABILITY OF RECORDS

11.1 Business Associate shall make its internal practices, books and records relating to the Use and Disclosure of Protected Health Information received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary for purposes of determining Covered Entity's compliance with the Privacy and Security Regulations.

11.2 Unless prohibited by the Secretary, Business Associate shall immediately notify Covered Entity of any requests made by the Secretary and provide Covered Entity with copies of any documents produced in response to such request.

12. MITIGATION OF HARMFUL EFFECTS

12.1 Business Associate shall mitigate, to the extent practicable, any harmful effect of a Use or Disclosure of Protected Health Information by Business Associate in violation of the requirements of this Business Associate Agreement that is known to Business Associate.

13. BREACH NOTIFICATION TO INDIVIDUALS

13.1 Business Associate shall, to the extent Covered Entity determines that there has been a Breach of Unsecured Protected Health Information by Business Associate, its employees, representatives, agents or Subcontractors, provide breach notification to the Individual in a manner that permits Covered Entity to comply with its obligations under 45 C.F.R. § 164.404.

13.1.1 Business Associate shall notify, subject to the review and approval of Covered Entity, each Individual whose Unsecured Protected Health Information has been, or is reasonably believed to have been, accessed, acquired, Used or Disclosed as a result of any such Breach.

13.1.2 The notification provided by Business Associate shall be written in plain language, shall be subject to review and approval by Covered Entity and shall include, to the extent possible:

(a) A brief description of what happened, including the date of the Breach and the date of the Discovery of the Breach, if known;

(b) A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(c) Any steps the Individual should take to protect him or herself from potential harm resulting from the Breach;

(d) A brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individual(s) and to protect against any further Breaches; and

(e) Contact procedures for Individual(s) to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site or postal address.

13.2 Covered Entity, in its sole discretion, may elect to provide the notification required by Section 13.1 and/or to establish the contact procedures described in Section 13.1.2.

13.3 Business Associate shall reimburse Covered Entity any and all costs incurred by Covered Entity, in complying with Subpart D of 45 C.F.R. Part 164, including but not limited to costs of notification, internet posting or media publication, as a result of Business Associate's Breach of Unsecured Protected Health Information; Covered Entity shall not be responsible for any costs incurred by Business Associate in providing the notification required by 13.1 or in establishing the contact procedures required by Section 13.1.2.

14. INDEMNIFICATION

14.1 Business Associate shall indemnify, defend, and hold harmless Covered Entity, its Special Districts, elected and appointed officers, employees, agents and volunteers from and against any and all liability, including but not limited to demands, claims, actions, fees, costs, expenses (including attorney and expert witness fees) and penalties and/or fines (including regulatory penalties and/or fines), arising from or connected with Business Associate's acts and/or omissions arising from and/or relating to this Business Associate Agreement, including, but not limited to, compliance and/or enforcement actions and/or activities, whether formal or informal, by the Secretary or by the Attorney General of the State of California.

14.2 Section 14.1 is not intended by the parties to limit in any way the scope of Business Associate's obligations related to Insurance and/or Indemnification in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

15. OBLIGATIONS OF COVERED ENTITY

15.1 Covered Entity shall notify Business Associate of any current or future restrictions or limitations on the Use or Disclosure of Protected Health Information that would affect Business Associate’s performance of the Services, and Business Associate shall thereafter restrict or limit its own Uses and Disclosures accordingly.

15.2 Covered Entity shall not request Business Associate to Use or Disclose Protected Health Information in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except to the extent that Business Associate may Use or Disclose Protected Health Information as provided in Sections 2.3, 2.5 and 2.6.

16. TERM

16.1 Unless sooner terminated as set forth in Section 17, the term of this Business Associate Agreement shall be the same as the term of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

16.2 Notwithstanding Section 16.1, Business Associate's obligations under Sections 11, 14 and 18 shall survive the termination or expiration of this Business Associate Agreement and the Agreement.

17. TERMINATION FOR CAUSE

17.1 In addition to and notwithstanding the termination provisions set forth in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, if either party determines that the other party has violated a material term of this Business Associate Agreement, and the breaching party has not cured the breach or ended the violation within the time specified by the non-breaching party, which shall be reasonable given the nature of the breach and/or violation, the non-breaching party may terminate this Business Associate Agreement.

17.2 In addition to and notwithstanding the termination provisions set forth in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, if either party determines that the other party has violated a material term of this Business Associate Agreement, and cure is not feasible, the non-breaching party may terminate this Business Associate Agreement immediately.

18. DISPOSITION OF PROTECTED HEALTH INFORMATION UPON TERMINATION OR EXPIRATION

18.1 Except as provided in Section 18.3, upon termination for any reason or expiration of this Business Associate Agreement, Business Associate shall return or, if agreed to by Covered entity, shall destroy as provided for in Section 18.2, all Protected Health Information received from Covered Entity, or created, maintained or received by Business Associate on behalf of Covered Entity, that Business Associate, including any Subcontractor, still maintains in any form. Business Associate shall retain no copies of the Protected Health Information.

18.2 Destruction for purposes of Section 18.2 and Section 6.6 shall mean that media on which the Protected Health Information is stored or recorded has been destroyed and/or electronic media have been cleared, purged, or destroyed in accordance with the use of a technology or methodology specified by the Secretary in guidance for rendering Protected Health Information unusable, unreadable or indecipherable to unauthorized individuals.

18.3 Notwithstanding Section 18.1, in the event that return or destruction of Protected Health Information is not feasible or Business Associate determines that any such Protected Health Information is necessary for Business Associate to continue its

proper management and administration or to carry out its legal responsibilities, Business Associate may retain that Protected Health Information for which destruction or return is infeasible or that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities and shall return or destroy all other Protected Health Information.

18.3.1 Business Associate shall extend the protections of this Business Associate Agreement to such Protected Health Information, including continuing to use appropriate safeguards and continuing to comply with Subpart C of 45 C.F.R Part 164 with respect to Electronic Protected Health Information, to prevent the Use or Disclosure of such information other than as provided for in Sections 2.5 and 2.6 for so long as such Protected Health Information is retained, and Business Associate shall not Use or Disclose such Protected Health Information other than for the purposes for which such Protected Health Information was retained.

18.3.2 Business Associate shall return or, if agreed to by Covered entity, destroy the Protected Health Information retained by Business Associate when it is no longer needed by Business Associate for Business Associate's proper management and administration or to carry out its legal responsibilities.

18.4 Business Associate shall ensure that all Protected Health Information created, maintained, or received by Subcontractors is returned or, if agreed to by Covered entity, destroyed as provided for in Section 18.2.

19. AUDIT, INSPECTION AND EXAMINATION

19.1 Covered Entity reserves the right to conduct a reasonable inspection of the facilities, systems, information systems, books, records, agreements and policies and procedures relating to the Use or Disclosure of Protected Health Information for the purpose determining whether Business Associate is in compliance with the terms of this Business Associate Agreement and any non-compliance may be a basis for termination of this Business Associate Agreement and the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, as provided for in Section 17.

19.2 Covered Entity and Business Associate shall mutually agree in advance upon the scope, timing and location of any such inspection.

19.3 At Business Associate's request, and to the extent permitted by law, Covered Entity shall execute a nondisclosure agreement, upon terms and conditions mutually agreed to by the parties.

19.4 That Covered Entity inspects, fails to inspect or has the right to inspect as provided for in Section 19.1 does not relieve Business Associate of its responsibility to comply with this Business Associate Agreement and/or the HIPAA Rules or impose on Covered Entity any responsibility for Business Associate's compliance with any applicable HIPAA Rules.

19.5 Covered Entity's failure to detect, its detection but failure to notify Business Associate, or its detection but failure to require remediation by Business Associate of an unsatisfactory practice by Business Associate, shall not constitute

acceptance of such practice or a waiver of Covered Entity's enforcement rights under this Business Associate Agreement or the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

19.6 Section 19.1 is not intended by the parties to limit in any way the scope of Business Associate's obligations related to Inspection and/or Audit and/or similar review in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

20. MISCELLANEOUS PROVISIONS

20.1 Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with the terms and conditions of this Business Associate Agreement will be adequate or satisfactory to meet the business needs or legal obligations of Business Associate.

20.2 HIPAA Requirements. The parties agree that the provisions under HIPAA Rules that are required by law to be incorporated into this Amendment are hereby incorporated into this Agreement.

20.3 No Third Party Beneficiaries. Nothing in this Business Associate Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

20.4 Construction. In the event that a provision of this Business Associate Agreement is contrary to a provision of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, the provision of this Business Associate Agreement shall control. Otherwise, this Business Associate Agreement shall be construed under, and in accordance with, the terms of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

20.5 Regulatory References. A reference in this Business Associate Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

20.6 Interpretation. Any ambiguity in this Business Associate Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Rules.

20.7 Amendment. The parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the HIPAA Rules and any other privacy laws governing Protected Health Information.

BUSINESS ASSOCIATE LISTING

Business Associate Name: _____

Type of Services Provided: _____

Website URL: _____

First Point of Contact

Title: _____

Name: _____

Address: _____

Phone: _____

E-mail: _____

Second Point of Contact

Title: _____

Name: _____

Address: _____

Phone: _____

E-mail: _____

SCHEDULE 4
ADDITIONAL INSURANCE REQUIREMENTS

In addition to, and subject to, the requirements and any other provisions of the Master Agreement relating to insurance, Contractor shall provide and maintain for the term of the Work Order executed under the Master Agreement and thereafter, to the extent required herein, the insurance coverage(s) specified below. As used herein, the term "County and its Agents" shall mean and refer to the County of Los Angeles and its Special Districts, Elected Officials, Officers, Agents, Employees and Volunteers.

1. PRIVACY/NETWORK SECURITY (CYBER) LIABILITY INSURANCE

Contractor shall secure and maintain cyber liability insurance coverage with limits of $10 million per occurrence and in the aggregate during the term of the Work Order executed pursuant to the Master Agreement, including coverage for: network security liability; privacy liability; privacy regulatory proceeding, defense, response, expenses and fines; technology professional liability (errors and omissions); privacy breach expense reimbursement (liability arising from the loss or disclosure of County Information no matter how it occurs); system breach; denial or loss of service; introduction, implantation, or spread of malicious software code; unauthorized access to or use of computer systems; and Data/Information loss and business interruption; any other liability or risk that arises out of the Master Agreement. Contractor shall add the County as an additional insured to its cyber liability insurance policy and provide to County certificates of insurance evidencing the foregoing upon County's request. The procuring of the insurance described herein, or delivery of the certificates of insurance described herein, shall not be construed as a limitation upon Contractor's liability or as full performance of its indemnification obligations hereunder. No exclusion/restriction for unencrypted portable devices/media may be on the policy.