STANDARD EXHIBITS

B BUDGET (NOT ATTACHED TO CONTRACT)

C FISCAL PROVISIONS AND INVOICE

D COUNTY'S ADMINISTRATION

E CONTRACTOR'S ADMINISTRATION

F FORMS REQUIRED AT THE TIME OF CONTRACT EXECUTION F1-F2
CONTRACTOR/EMPLOYEE ACKNOWLEDGEMENT AND
CONFIDENTIALITY AGREEMENT

G SAFELY SURRENDERED BABY LAW

UNIQUE EXHIBITS

FORMS REQUIRED AT THE COMPLETION OF THE CONTRACTS INVOLVING INTELLECTUAL PROPERTY DEVELOPED/DESIGNED BY CONTRACTOR

I BUSINESS ASSOCIATE AGREEMENT UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

J CHARITABLE CONTRIBUTIONS CERTIFICATION

Q INFORMATION SECURITY AND PRIVACY REQUIREMENTS

R CONTRACTOR COMPLIANCE WITH INFORMATION SECURITY REQUIREMENTS

T ELECTRONIC DATA TRANSMISSION TRADING PARTNER

U ATTESTATION REGARDING INFORMATION SECURITY REQUIREMENTS

BUDGET

NOT ATTACHED TO CONTRACT

1. PAYMENT PROCEDURES

Contractor shall submit monthly invoices **TF-CBT Training Cost Invoice** - Attachment I, for actual cost incurred for services provided per Exhibit A - SOW. Contractor must submit supporting documentation, and receipts (if applicable), for the confirmation and verification of services and invoice approval. Invoices shall be specific as to the type of services being provided.

DMH shall make reimbursements payable to Contractor. DMH shall send payments to:

Contractor:

Contractor Address:

City, State, Zip:

2. DESIGNATED DMH CONTACT PERSON

All questions and correspondence should be directed to:

Contact Name:
Los Angeles County Department of Mental Health
Address: 510 S. Vermont Avenue, Los Angeles, CA 90020
Phone Number:

Invoices should be directed to:

Contact Name:
Address: 510 South Vermont Avenue, Los Angeles, CA 90020
Email: _____

Date of Invoice:
TF-CBT TRAINING INVOICE FORM

Section 1 - PRE-TRAINING VIDEO			
Trainer	**Training Date**	**Description**	**Cost**
			$0.00

Section 2 - INITIAL TRAINING			
Trainer	**Training Date**	**Description**	**Cost**
			$0.00

Section 3 - TECHNICAL ASSISTANCE CALLS			
Trainer	**Training Date**	**Description**	**Cost**
			$0.00

Section 4 - BOOSTER TRAINING			
Trainer	**Training Date**	**Description**	**Cost**
			$0.00

Section 5 - AUDIO REVIEWS			
Trainer	**Training Date**	**Description**	**Cost**
			$0.00

Section 6 - MISCELLANEOUS		
Type	**Description**	**Cost**
		$0.00
	TOTAL REIMBURSEMENT REQUESTED:	**$0.00**

I hereby certify that all the information contained above is true and accurate to the best of my knowledge.

Contractor's Name:	
Contractor's Signature:	

DMH APPROVAL		
Comments:		Amount Approved: Amount Denied:
Department of Mental Health Approval	Approved by (Signature)	Date
	Print Name	Title

COUNTY'S ADMINISTRATION

CONTRACT NO. _____

COUNTY'S PROJECT DIRECTOR:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

Facsimile: _____

E-mail Address: _____

COUNTY'S PROJECT MANAGER:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

Facsimile: _____

E-mail Address: _____

COUNTY'S PROJECT MONITOR:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

Facsimile: _____

E-mail Address: _____

CONTRACTOR'S ADMINISTRATION

CONTRACTOR'S NAME: _____

CONTRACT NO. _____

CONTRACTOR'S PROJECT MANAGER:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

Facsimile: _____

E-mail Address: _____

CONTRACTOR'S AUTHORIZED OFFICIAL(S):

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

Facsimile: _____

E-mail Address: _____

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

Facsimile: _____

E-mail Address: _____

NOTICES TO CONTRACTOR:

Name: _____

Title: _____

Address: _____

_____

Telephone: _____

Facsimile: _____

E-mail Address: _____

FORMS REQUIRED AT THE TIME OF CONTRACT EXECUTION

F1 CONTRACTOR ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

F2 CONTRACTOR EMPLOYEE ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

CONTRACTOR ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

Contractor Name: _____ Contract No _____

GENERAL INFORMATION:

The Contractor referenced above has entered into a contract with the County of Los Angeles to provide certain services to the County. The County requires the Corporation to sign this Contractor Acknowledgement and Confidentiality Agreement.

CONTRACTOR ACKNOWLEDGEMENT:

Contractor understands and agrees that the Contractor employees, consultants, Outsourced Vendors and independent contractors (Contractor's Staff) that will provide services in the above referenced agreement are Contractor's sole responsibility. Contractor understands and agrees that Contractor's Staff must rely exclusively upon Contractor for payment of salary and any and all other benefits payable by virtue of Contractor's Staff's performance of work under the above-referenced contract.

Contractor understands and agrees that Contractor's Staff are not employees of the County of Los Angeles for any purpose whatsoever and that Contractor's Staff do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced contract. Contractor understands and agrees that Contractor's Staff will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

CONFIDENTIALITY AGREEMENT:

Contractor and Contractor's Staff may be involved with work pertaining to services provided by the County of Los Angeles and, if so, Contractor and Contractor's Staff may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, Contractor and Contractor's Staff may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. Contractor and Contractor's Staff understand that if they are involved in County work, the County must ensure that Contractor and Contractor's Staff, will protect the confidentiality of such data and information. Consequently, Contractor must sign this Confidentiality Agreement as a condition of work to be provided by Contractor's Staff for the County.

Contractor and Contractor's Staff hereby agrees that they will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced contract between Contractor and the County of Los Angeles. Contractor and Contractor's Staff agree to forward all requests for the release of any data or information received to County's Project Manager.

Contractor and Contractor's Staff agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information and all other original materials produced, created, or provided to Contractor and Contractor's Staff under the above-referenced contract. Contractor and Contractor's Staff agree to protect these confidential materials against disclosure to other than Contractor or County employees who have a need to know the information. Contractor and Contractor's Staff agree that if proprietary information supplied by other County vendors is provided to me during this employment, Contractor and Contractor's Staff must keep such information confidential.

Contractor and Contractor's Staff agree to report any and all violations of this agreement by Contractor and Contractor's Staff and/or by any other person of whom Contractor and Contractor's Staff become aware.

Contractor and Contractor's Staff acknowledge that violation of this agreement may subject Contractor and Contractor's Staff to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

SIGNATURE: _____ DATE: _____

PRINTED NAME: _____

POSITION: _____

CONTRACTOR EMPLOYEE ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

Contractor Name: _____ Contract No _____

Employee Name: _____

GENERAL INFORMATION:

Your employer referenced above has entered into a contract with the County of Los Angeles to provide certain services to the County. The County requires your signature on this Contractor Employee Acknowledgement and Confidentiality Agreement.

EMPLOYEE ACKNOWLEDGEMENT:

I understand and agree that the Contractor referenced above is my sole employer for purposes of the above-referenced contract. I understand and agree that I must rely exclusively upon my employer for payment of salary and any and all other benefits payable to me or on my behalf by virtue of my performance of work under the above-referenced contract.

I understand and agree that I am not an employee of the County of Los Angeles for any purpose whatsoever and that I do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced contract. I understand and agree that I do not have and will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

I understand and agree that I may be required to undergo a background and security investigation(s). I understand and agree that my continued performance of work under the above-referenced contract is contingent upon my passing, to the satisfaction of the County, any and all such investigations. I understand and agree that my failure to pass, to the satisfaction of the County, any such investigation will result in my immediate release from performance under this and/or any future contract.

CONFIDENTIALITY AGREEMENT:

I may be involved with work pertaining to services provided by the County of Los Angeles and, if so, I may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, I may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. I understand that if I am involved in County work, the County must ensure that I, too, will protect the confidentiality of such data and information. Consequently, I understand that I must sign this agreement as a condition of my work to be provided by my employer for the County. I have read this agreement and have taken due time to consider it prior to signing.

I hereby agree that I will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced contract between my employer and the County of Los Angeles. I agree to forward all requests for the release of any data or information received by me to my immediate supervisor.

I agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information and all other original materials produced, created, or provided to or by me under the above-referenced contract. I agree to protect these confidential materials against disclosure to other than my employer or County employees who have a need to know the information. I agree that if proprietary information supplied by other County vendors is provided to me during this employment, I must keep such information confidential.

I agree to report to my immediate supervisor any and all violations of this agreement by myself and/or by any other person of whom I become aware. I agree to return all confidential materials to my immediate supervisor upon completion of this contract or termination of my employment with my employer, whichever occurs first.

SIGNATURE: _____ DATE: _____

PRINTED NAME: _____

POSITION: _____


THERE'S A BETTER CHOICE.
SAFELY SURRENDER YOUR BABY.
Any fire station. Any hospital. Any time.
1.877.222.9723
BabySafeLA.org
No shame | No blame | No names
21
FIRE STATION
98

Some parents of newborns can find themselves in difficult circumstances. Sadly, babies are sometimes harmed or abandoned by parents who feel that they're not ready or able to raise a child. Many of these mothers or fathers are afraid and don't know where to turn for help.

This is why California has a Safely Surrendered Baby Law, which gives parents the choice to legally leave their baby at any hospital or fire station in Los Angeles County.

FIVE THINGS YOU NEED TO KNOW ABOUT BABY SAFE SURRENDER

1. Your newborn can be surrendered at any hospital or fire station in Los Angeles County up to 72 hours after birth.
2. You must leave your newborn with a fire station or hospital employee.
3. You don't have to provide your name.
4. You will only be asked to voluntarily provide a medical history.
5. You have 14 days to change your mind; a matching bracelet (parent) and anklet (baby) are provided to assist you if you change your mind.

No shame | No blame | No names

BabySafeLA.org

ABOUT THE BABY SAFE SURRENDER PROGRAM

In 2002, a task force was created under the guidance of the Children's Planning Council to address newborn abandonment and to develop a strategic plan to prevent this tragedy.

Los Angeles County has worked hard to ensure that the Safely Surrendered Baby Law prevents babies from being abandoned. We're happy to report that this law is doing exactly what it was designed to do: save the lives of innocent babies. Visit BabySafeLA.org to learn more.

No shame | No blame | No names

ANY FIRE STATION.
ANY HOSPITAL.
ANY TIME.

1.877.222.9723
BabySafeLA.org

THERE'S A BETTER CHOICE.
SAFELY SURRENDER YOUR BABY.

BabySafeLA.org

No shame | No blame | No names

FROM SURRENDER TO ADOPTION: ONE BABY'S STORY

Los Angeles County firefighter Ted and his wife Becki were already parents to two boys. But when they got the call asking if they would be willing to care for a premature baby girl who'd been safely surrendered at a local hospital, they didn't hesitate.

Baby Jenna was tiny, but Ted and Becki felt lucky to be able to take her home. "We had always wanted to adopt," Ted says, "but taking home a vulnerable safely surrendered baby was even better. She had no one, but now she had us. And, more importantly, we had her."

Baby Jenna has filled the longing Ted and Becki had for a daughter—and a sister for their boys. Because her birth parent safely surrendered her when she was born, Jenna is a thriving young girl growing up in a stable and loving family.

ANSWERS TO YOUR QUESTIONS

Who is legally allowed to surrender the baby?
Anyone with lawful custody can drop off a newborn within the first 72 hours of birth.

Do you need to call ahead before surrendering a baby?
No. A newborn can be surrendered anytime, 24 hours a day, 7 days a week, as long as the parent or guardian surrenders the child to an employee of the hospital or fire station.

What information needs to be provided?
The surrendering adult will be asked to fill out a medical history form, which is useful in caring for the child. The form can be returned later and includes a stamped return envelope. No names are required.

What happens to the baby?
After a complete medical exam, the baby will be released and placed in a safe and loving home, and the adoption process will begin.

What happens to the parent or surrendering adult?
Nothing. They may leave at any time after surrendering the baby.

How can a parent get a baby back?
Parents who change their minds can begin the process of reclaiming their baby within 14 days by calling the Los Angeles County Department of Children and Family Services at (800) 540-4000.

If you're unsure of what to do:
You can call the hotline 24 hours a day, 7 days a week and anonymously speak with a counselor about your options or have your questions answered.

1.877.222.9723 or BabySafeLA.org
English, Spanish and 140 other languages spoken.

BUSINESS ASSOCIATE AGREEMENT UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("HIPAA")

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 (“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, the "HIPAA Rules").

Contractor performs or provides functions, activities or services to County that require Contractor in order to provide such functions, activities or 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 ("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" will 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" will 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, 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 will 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, or services 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 will 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 must 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 must 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 must 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 must 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 must 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 must 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 must 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 this Agreement of which Business Associate becomes aware.

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

5.1.3. Business Associate must 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 will 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 must 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 must 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 knowledge of the facts and circumstances of the non-

permitted Use or Disclosure of PHI, Security Incident, or Breach

5.2.2 Business Associate must 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 and 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 themselves 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 knowledge 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 must 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 must 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 must 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 must 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 must 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 must 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 must immediately notify County.

6.5 Without limiting the requirements of Section 6.1, the agreement required by Section 6.1 (Subcontractor Business Associate Agreement) must 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) must 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 must 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 must, 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 must 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 must notify Covered Entity in writing within two (2) days of the receipt of the request. Whether access will be provided or denied will 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 must 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 must, 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 must notify Covered Entity in writing within five (5) days of the receipt of the request. Whether an amendment will be granted or denied will be determined by Covered Entity.

9. ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

9.1 Business Associate must 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 must 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 must document the information specified in Section 9.1.1, and must maintain the information for six (6) years from the date of the Disclosure.

9.2 Business Associate must 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 must notify Covered Entity in writing within five (5) days of the receipt of the request, and must provide the requested accounting of disclosures to the Individual(s) within 30 days. The information provided in the accounting must 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 must comply with the requirements of Subpart E that apply to Covered Entity's performance of such obligation(s).

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

11. AVAILABILITY OF RECORDS

11.1 Business Associate must 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 must 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 must 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 must, 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 must 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 must be written in plain language, will be subject to review and approval by Covered Entity, and must 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 themselves 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, including 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 must 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 will 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 must indemnify, defend, and hold harmless Covered Entity, its Special Districts, elected and appointed officers, employees, and agents 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 will 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 must thereafter restrict or limit its own Uses and Disclosures accordingly.

15.2 Covered Entity will 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 will 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 will survive the termination or expiration of this Business Associate 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 must 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 must return or, if agreed to by Covered entity, must 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 will retain no copies of the Protected Health Information.

18.2 Destruction for purposes of Section 18.2 and Section 6.6 will 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 must return or destroy all other Protected Health Information.

18.3.1 Business Associate must 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 must 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 must 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 must 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 will 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 will 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, will 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 will 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 will control. Otherwise, this Business Associate Agreement will 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 will 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.

CHARITABLE CONTRIBUTIONS CERTIFICATION

Company Name

Address

Internal Revenue Service Employer Identification Number

California Registry of Charitable Trusts "CT" number (if applicable)

The Nonprofit Integrity Act (SB 1262, Chapter 919) added requirements to California's Supervision of Trustees and Fundraisers for Charitable Purposes Act which regulates those receiving and raising charitable contributions.

Check the Certification below that is applicable to your company.

☐ Proposer or Contractor has examined its activities and determined that it does not now receive or raise charitable contributions regulated under California's Supervision of Trustees and Fundraisers for Charitable Purposes Act. If Bidder engages in activities subjecting it to those laws during the term of a County contract, it will timely comply with them and provide County a copy of its initial registration with the California State Attorney General's Registry of Charitable Trusts when filed.

OR

☐ Proposer or Contractor is registered with the California Registry of Charitable Trusts under the CT number listed above and is in compliance with its registration and reporting requirements under California law. Attached is a copy of its most recent filing with the Registry of Charitable Trusts as required by Title 11 California Code of Regulations, sections 300-301 and Government Code sections 12585-12586.

Signature:_____ Date: _____

Printed Name: _____ Title: _____

INFORMATION SECURITY AND PRIVACY REQUIREMENTS FOR CONTRACTS

The County of Los Angeles ("County") is committed to safeguarding the Integrity of County Systems, Data, and Information, and to protecting the privacy rights of the individuals that it serves. This Information Security and Privacy Requirements Exhibit ("Exhibit") sets forth the County and the Contractor's commitment and agreement to fulfill each of their obligations under applicable State or federal laws, rules, or 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 the Contractor before the Effective Date of the Contract 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 base agreement between the County and Contractor (the "Contract") and any other agreements between the parties. However, it is the 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 the Contractor, entitling the 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 the 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 the 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 the 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 Los Angeles County, is under the direct control of Los Angeles County, whether or not they are paid by Los Angeles 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 the County.

2. INFORMATION SECURITY AND PRIVACY PROGRAMS

a. **Information Security Program.** The Contractor shall maintain a company-wide Information Security Program designed to evaluate Risks to the Confidentiality, Availability, and Integrity of the County Information covered under this 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, compliance with all applicable laws and regulations, and addresses new and emerging Threats and Risks.

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

- Protect the Confidentiality, Integrity, and Availability of County Information in the 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, or 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. The 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. The 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. The 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. The Contractor's Privacy Program shall include performing ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

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

The Contractor's Privacy Program shall include:

- A Privacy Program framework that identifies and ensures that the 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 the County, and the County shall retain exclusive rights and ownership thereto. County Information shall not be used by the 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 the Contractor, or commercially exploited or otherwise used by, or on behalf of, the Contractor, its officers, directors, employees, or agents. The Contractor may assert no lien on or right to withhold from the County, any County Information it receives from, receives addressed to, or stores on behalf of, the County. Notwithstanding the foregoing, the 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 the Contractor, provided that (i) no County Information in such aggregated or compiled pool is identifiable as originating from, or can be traced back to the

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. The Contractor specifically consents to the 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

The Contractor may use County Information only as necessary to carry out its obligations under the Contract. The 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

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

b. **Disclosure of County Information.** The 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 the County's Contract administrator in consultation with the 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, the Contractor shall notify the County's Contract administrator immediately and prior to any such disclosure, to provide the 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, the Contractor may encounter County non-public information ("NPI"), 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.

The Contractor shall not disclose or publish any County NPI and/or material received or used in performance of the Contract. This obligation is perpetual.

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

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

7. CONTRACTOR EMPLOYEES

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

The Contractor shall supply each of its employees with appropriate annual training regarding Information Security procedures, Risks, and Threats. The 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:** The Contractor's Privacy Policies and procedures as described in Section 2b above, Privacy Program.

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

8. SUBCONTRACTORS AND THIRD PARTIES

The County acknowledges that in the course of performing its services, the 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. The 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 the 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) the 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.

The Contractor shall obtain advanced approval from the County's Chief Information Security Officer and/or Chief Privacy Officer prior to subcontracting 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, the 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 the County's Chief Information Security Officer.

The Contractor will encrypt County Information transmitted on networks outside of the Contractor's control with Transport Layer Security (TLS) 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.

In addition, the Contractor shall not store County Information in the cloud or in any other online storage provider without written authorization from the 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 the County's Chief Information Security Officer.

10. RETURN OR DESTRUCTION OF COUNTY INFORMATION

The 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 the 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 the 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 the 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 the County requests be returned to the County, the Contractor shall provide a written attestation on company letterhead certifying that all documents and materials have been delivered to the County. For documents or materials referred to in Subsections (i) and (ii) of this Section that the County requests be destroyed, the 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 the County's request, the Contractor shall return all hardware, if any, provided by the County to the Contractor. The hardware should be physically sealed and returned via a bonded courier, or as otherwise directed by the County.

b. **Method of Destruction.** The 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 the County Information cannot be retrieved. The Contractor will provide an attestation on company letterhead and certified documentation from a media destruction firm, detailing the destruction method used and the 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 10 days of termination or expiration of the Contract or at any time upon the County's request. On termination or expiration of this Contract, the County will return or destroy all Contractor's Information marked as confidential (excluding items licensed to the County hereunder, or that provided to the County by the Contractor hereunder), at the County's option.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

All Contractor facilities that process County Information will 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 will 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

The 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 below, SECURITY AND PRIVACY INCIDENTS; (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.

The Contractor must have 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 the Contractor makes backups to removable media (as described in Section 9 above, 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 above, 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 the County Project Director or Project Manager in writing; and (ii) if transferred using removable media (as described in Section 9 above, STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be sent via a bonded courier and protected using encryption technology designated by the Contractor and approved by the County's Chief Information Security Officer in writing. The foregoing requirements shall apply to back-up media stored by the Contractor at off-site facilities.

The 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 including, but not limited to, multi-factor authentication, use of virtual private networks (VPN), authorization, and event logging;

c. The Contractor will conduct regular, no less often 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. The Contractor shall record, review and act upon all events in accordance with Incident response policies set forth in Section 14 below, SECURITY AND PRIVACY INCIDENTS; and

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

14. SECURITY AND PRIVACY INCIDENTS

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

a. Promptly notify the County's Chief Information Security Officer, the Departmental Information Security Officer, and the County's Chief Privacy Officer of any Incidents involving County Information, within 24 hours of detection of the Incident. All notifications shall be submitted via encrypted email and telephone.

Chief Information Security Officer:
Jeffrey Aguilar
Chief Information Security Officer
320 W Temple, 7th Floor
Los Angeles, CA 90012
Phone: (213) 253-5659

Chief Privacy Officer:
Lillian Russell
Chief Privacy Officer
320 W Temple, 7th Floor
Los Angeles, CA 90012
Phone: (213) 351-5363

County Chief Information Security Officer and Chief Privacy Officer email
CISO-CPO_Notify@lacounty.gov

DMH Departmental Information Security Officer:
James Thurmond
DMH Departmental Information Security
Officer 510 S. Vermont Avenue, 16th Floor
Los Angeles, CA 90020
Phone: (213) 435-5937
DMH Departmental Information Security Officer email:
InformationSecurity@dmh.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;

(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; and

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

c. Cooperate with the County to investigate the Incident and seek to identify the specific County Information involved in the Incident upon the County's

request, without charge, unless the Incident was caused by the acts or omissions of the County. As Information about the Incident is collected or otherwise becomes available to the Contractor, and unless prohibited by law, the Contractor shall provide Information regarding the nature and consequences of the Incident that are reasonably requested by the County.

d. Immediately initiate the appropriate portions of their 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, the County, law firms, and and/or law enforcement agencies at the direction of the County to help determine the nature, extent, and source of any Incident, and reasonably assist and cooperate with the County on any additional disclosures that the County is required to make as a result of the Incident.

f. Allow the County, or its third-party designee at the County's election, to perform audits and tests of the Contractor's environment that may include, but are not limited to, interviews of relevant employees, reviews of documentation, or technical inspections 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/or this Exhibit, the 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.

15. NON-EXCLUSIVE EQUITABLE REMEDY

The 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 the County, and therefore, that upon any such breach, the 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 above, CONFIDENTIALITY, shall constitute a material breach of the Contract and be grounds for immediate termination of the Contract in the exclusive discretion of the County.

16. AUDIT AND INSPECTION

a. Self-Audits. The 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 the County.

The 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. The Contractor shall provide the audit results and any corrective action documentation to the County promptly upon audit completion, at the County's request. With respect to any other report, certification, or audit or test results prepared or received by the Contractor that contains any County Information, the Contractor shall promptly provide the County with copies of the same upon the County's reasonable request, including identification of any failure or exception in the Contractor's Information systems, products, and services, and the corresponding steps taken by the Contractor to mitigate such failure or exception. Any reports and related materials provided to the County pursuant to this Section shall be provided at no additional charge to the County.

b. **County Requested Audits.** At its own expense, the County, or an independent third-party auditor commissioned by the County, shall have the right to audit the 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 the County's request, the Contractor shall complete a questionnaire regarding Contractor's Information Security and/or program. The County shall pay for the County requested audit unless the auditor finds that the Contractor has materially breached this Exhibit, in which case the Contractor shall bear all costs of the audit; and if the audit reveals material non-compliance with this Exhibit, the County may exercise its termination rights under the Contract.

Such audit shall be conducted during the Contractor's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect the Contractor's normal business operations. The 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. The Contractor shall cooperate with the 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 the County. The Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

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

actions or modifications, if any, the Contractor will implement in response to such audits.

17. CYBER LIABILITY INSURANCE

The 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. The Contractor shall secure and maintain cyber liability insurance coverage with limits of at least $2 million 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 the Contract. The Contractor shall add the County as an additional insured to its cyber liability insurance policy and provide to the County certificates of insurance evidencing the foregoing upon the 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 the 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, the Contractor agrees to indemnify, defend, and hold harmless the 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 :

- The Contractor's violation of any federal and State laws in connection with its accessing, collecting, processing, storing, disclosing, or otherwise using County Information;

- The Contractor's failure to perform or comply with any terms and conditions of the Contract or related agreements with the 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 the 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, the 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 County shall be entitled 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.

19. CERTIFICATION

Within 10 business days of the receipt of this document, Contractor must complete and provide to County the Exhibit R "DMH Contractor's Compliance with Information Security Requirements" questionnaire (for itself and on behalf of its subcontractors) certifying that will be compliant with Los Angeles County Board of Supervisors' Policies and attest that it has implemented adequate controls to meet the expected Information Security minimum standard set forth above, at the commencement and during the term of the Contract.

In addition, Contractor must be prepared to provide supporting evidence upon request to validate its compliance. Failure on the part of the Contractor to comply with any of the provisions of this Exhibit, "Information Security and Privacy Requirements for Contracts" shall constitute a material breach of this arrangement upon which the County may terminate or suspend the Contract.

20. REPORTING REQUIREMENTS FOR SIGNIFICANT CHANGES

During the term of the Contract, Contractor must notify the County within 10 days of implementation, in writing, about any significant changes such as technology changes, modification in the implemented security safeguards or any major infrastructure changes. Depending on the change(s), Contractor may be asked to re-submit Exhibit R, "DMH Contractor's Compliance with Information Security Requirements".

21. MAINTAINING COMPLIANCE

Contractor must provide updates about its information security practices **annually** by completing Exhibit R "DMH Contractor's Compliance with Information Security Requirements" questionnaire. By submitting, Contractor certifies that its implemented controls will continue to be in compliance with Los Angeles County

Board of Supervisors' Policies, and the expected minimum standard set forth above during the term of any arrangement that may be awarded pursuant to this agreement. The completed forms must be returned to DMH Information Security Officer (DISO) within 10 business days of receipt and must be approved for continuous business with the County.

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 to the Contractor, the 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 the County to use the full benefits of the SaaS and achieve the purposes stated therein.

b. **Business Continuity:** In the event that the Contractor's infrastructure containing or processing County Information becomes lost, altered, damaged, interrupted, destroyed, or otherwise limited in functionality in a way that affects the County's use of the SaaS, the Contractor shall immediately and within 24 hours, implement the Contractor's Business Continuity Plan, consistent with Section 12 of Exhibit Q, OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY, such that the Contractor can continue to provide full functionality of the SaaS as described in the Contract.

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

   The 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, the County Information may be accessed and retrieved within two hours at any point in time. To the extent the Contractor hosts County Information related to the SaaS, the Contractor shall create daily backups of all County Information related to the 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 this Contract and available when needed.

c. **Enhancements:** Upgrades, replacements and new versions: The 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 the 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, the Contractor shall promptly notify the County of any available updates, enhancements or newer versions of the SaaS and within 30 days update or provide the new version to the County. The Contractor shall provide any accompanying documentation in the form of new or revised documentation necessary

to enable the County to understand and use the enhanced, updated, or replaced SaaS.

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

d. **Location of County Information:** The 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. **Annual Data Center Audit and Certification:** The 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. The 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 the Contractor's plan for addressing or resolving the audit findings shall be shared with County's Chief Information Security Officer within 10 business days of the Contractor's receipt of the audit results. The 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, the Contractor shall notify County of the proposed subcontractor(s) and the purposes for which they may be engaged at least 30 days prior to engaging the Subcontractor, and obtain written consent of the County's Contract Administrator.

g. **Information Import Requirements at Termination:** Within one day of notification of termination of the Contract, the 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 90 day period prior to, and/or following the expiration or termination of the Contract, in whole or in part, the 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 the Contractor to a successor;

(ii) Providing reasonable training to County staff or a successor in the performance of the SaaS being performed by the Contractor;

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

(iv) Such other activities upon which the Parties may reasonably agree.

ADDENDUM B: CONTRACTOR HARDWARE CONNECTING TO COUNTY SYSTEMS

Notwithstanding any other provisions in the Contract, the Contractor shall ensure the following provisions and security controls are established for any and all Systems or Hardware provided under the Contract.

a. **Inventory:** The Contractor must actively manage, including through inventory, tracking, loss prevention, replacement, updating, and correcting, all hardware devices covered under the Contract. The Contractor must be able to provide such management records to the County at inception of the Contract and upon request thereafter.

b. **Access Control:** The Contractor agrees to manage access to all Systems or Hardware covered under the Contract. This includes industry-standard management of administrative privileges including, but not limited to, maintaining an inventory of administrative privileges, changing default passwords, use of unique passwords for each individual accessing Systems or Hardware under the Contract, and minimizing the number of individuals with administrative privileges to those strictly necessary. Prior to effective date of the Contract, the Contractor must document its access control plan for Systems or Hardware covered under the Contract and provide such plan to the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO) for review and approval. The Contractor must modify and/or implement such plan as directed by the DISO and CISO.

c. **Operating System and Equipment Hygiene**: The Contractor agrees to ensure that Systems or Hardware will be kept up to date, using only the most recent and supported operating systems, applications, and programs, including any patching or other solutions for vulnerabilities, within 90 days of the release of such updates, upgrades, or patches. The Contractor agrees to ensure that the operating system is configured to eliminate any unnecessary applications, services and programs. If for some reason the Contractor cannot do so within 90 days, the Contractor must provide a Risk assessment to the County's CISO.

d. **Vulnerability Management:** The Contractor agrees to continuously acquire, assess, and take action to identify and remediate vulnerabilities within the Systems and Hardware covered under this Contract. If such vulnerabilities cannot be addressed, The Contractor must provide a Risk assessment to the DISO who will consult with the CISO. The County's CISO must approve the Risk acceptance and the Contractor accepts liability for Risks that result to the County for exploitation of any un-remediated vulnerabilities.

e. **Media Encryption:** Throughout the duration of the Contract, the Contractor will encrypt all workstations, portable devices (e.g., mobile, wearables, tablets,) and removable media (e.g., portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) associated with Systems and Hardware provided under the Contract in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise required or approved by the County's CISO.

f. **Malware Protection:** The Contractor will provide and maintain industry-standard endpoint antivirus and antimalware protection on all Systems and Hardware as approved or required by the DISO who will consult with the County's CISO to ensure provided hardware is free and remains free of malware. The Contractor agrees to provide the County documentation proving malware protection status upon request.

ADDENDUM C: APPLICATION SOURCE CODE REPOSITORY

The Contractor shall manage the source code in the manner prescribed in this Addendum unless the Contract prescribes procedures for managing the source code and those procedures are no less stringent than the procedures described in this addendum.

a. **County Application Source Code.** To facilitate the centralized management, reporting, collaboration, and continuity of access to the most current production version of application source code, all code, artifacts, and deliverables produced under the Contract, (hereinafter referred to as "County Source Code") shall be version controlled, stored, and delivered on a single industry-standard private Git repository, provided, managed, and supported by the County. Upon commencement of the Contract period, the Contractor will be granted access to the County's private Git repository.

b. **Git Repository.** The Contractor will use the County Git repository during the entire lifecycle of the project from inception to final delivery. The Contractor will create and document design documents, Data flow diagrams, security diagrams, configuration settings, software or hardware requirements and specifications, attribution to third-party code, libraries and all dependencies, and any other documentation related to all County Source Code and corresponding version-controlled documentation within the Git repository. This documentation must include an Installation Guide and a User Guide for the final delivered source code such that County may download, install, and make full functional use of the delivered code as specified and intended.

DMH CONTRACTOR' S COMPLIANCE
WITH INFORMATION SECURITY REQUIREMENTS

Contractor Agency Name: _____

Contractor shall provide information about its information security practices by completing this Exhibit **annually**. By submitting this Exhibit, Contractor certifies that they will be compliant with Los Angeles County Board of Supervisors Policies and attest that it has implemented adequate controls to meet the following expected Information Security minimum standards, at the commencement and during the term of any awarded Contract. Contractor must be prepared to provide supporting evidence upon request. The completed forms must be returned to the DMH Information Security Officer (DISO) for approval within 10 business days from receipt. Any significant changes during the term of the Contract must be reported within 10 business days of implementation. Depending on the change(s), Contractor may be asked to re-submit this Exhibit.

COMPLIANCE QUESTIONS

					DOCUMENTATION AVAILABLE	
		YES	NO	N/A	YES	NO
1	Will County's non-public data stored on your workstation(s) be encrypted? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
2	Will County non-public data stored on your laptop(s) be encrypted? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
3	Will County's non-public data stored on removable media be encrypted? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
4	Will County non-public data be encrypted when transported? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
5	Will any validation/attestation reports generated by the encryption tools be maintained? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
6	Will County's non-public data be stored on remote servers*? *Cloud storage, Software-as-a-Service or SaaS *Please provide public URL and hosting information for the server.*	☐	☐	☐	☐	☐
7	Will all users with access to County's non-public data participate in an annual information security awareness training? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
8	Will County's non-public data residing on endpoints be protected by an up-to-date antivirus and/or anti-malware software? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐

To be completed and returned to DMH Information Security Officer within ten (10) business days from receipt of this document

		YES	NO	N/A	YES	NO
9	Will all endpoints accessing and/or storing County's non-public data be physically secured? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
10	Will all security incidents involving County's data be promptly reported? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
11	Will all users' access be formally authorized, and users provided with unique logon IDs & complex passwords for accessing County data? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
12	Will all users' activities be monitored to ensure they are accessing the minimum information necessary to perform their assignments? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
13	Will users' access be modified once their role no longer justifies such access, and/or promptly suspended upon discharge or termination? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
14	Will all endpoints accessing and/or storing County's non-public data be regularly patched and updated for known vulnerabilities? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
15	Will all endpoints accessing and/or storing County's non-public data be rendered unreadable and/or unrecoverable, prior to disposition? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
16	Will annual inspections and risk assessments be conducted on systems involving County data and will identified weaknesses and vulnerabilities be promptly mitigated or remediated? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
17	Does the entity have policies and procedures to ensure continuity and availability of critical business processes during emergencies or disasters and ability to restore/recover data from ransomware attacks? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐
18	Upon expiration or termination of the contractual agreement with the County, will Contractor return or destroy County's non-public data? *If "NO" or N/A, please explain.*	☐	☐	☐	☐	☐

Authorized Signatory Name (Print) | **Authorized Signatory Official Title**

Authorized Signatory Signature | **Date**

To be completed and returned to DMH Information Security Officer within ten (10) business days from receipt of this document

LOS ANGELES COUNTY
DEPARTMENT OF MENTAL HEALTH
hope. recovery. wellbeing.

CHIEF INFORMATION OFFICE BUREAU

ELECTRONIC DATA TRANSMISSION TRADING PARTNER EXHIBIT (TPE)

This Trading Partner Exhibit ('TPE') is made and entered by and between the Network Provider named _____ ("Trading Partner"), whose Network Provider number is _____ and the County of Los Angeles – Department of Mental Health ("DMH").

DMH and the Trading Partner will exchange information and data electronically in connection with certain healthcare transactions and the Trading Partner must be readily equipped at their own expense with the Systems and trained personnel necessary to engage in the successful exchange of electronic information and data. The electronic transmissions of information and data in addition to the confidentiality and security of the data exchanged between the parties, is of the highest priority.

1. DEFINITIONS

1.1 Agents
Third parties or organizations that contract with the Trading Partner to perform designated services in order to facilitate the electronic transfer or exchange of data. Examples of Agents include claims clearinghouses, vendors, and billing services.

1.2 Confidential Information
Information relating to specific Individuals which is exchanged between DMH, the Trading Partner, and/or the Agents for various business purposes, but which is protected from disclosure to unauthorized persons or entities by The Privacy Act of 1974, The Administrative Simplification Provisions of the federal Health Insurance Portability and Accountability Act ("HIPAA") and regulations promulgated thereunder; the Insurance Information and Privacy Protections Act, and/or other applicable State and federal statutes and regulations, which shall hereinafter be collectively referred to as "Privacy Statutes and Regulations."

1.3 Data
A formalized representation of specific facts or concepts suitable for communication, interpretation, or processing by people or by automatic means.

1.4 Data Log
A complete written summary of Data and Data Transmissions exchanged between the Parties over the period of time this TPE is in effect, including, without limitation, sender and receiver information, the date and time of transmission and the general nature of the transmission.

1.5 Data Transmission

The automated transfer or exchange of data between Trading Partners or their Agents, by means of their Systems which are compatible for that purpose, pursuant to the terms and conditions set forth in this TPE.

1.6 Electronic Data Interchange ("EDI")

The automated exchange of business data from application to application which utilizes an American National Standards Institute (ANSI) approved or other mutually agreed format.

1.7 Envelope

A control structure in a mutually agreed format for the electronic interchange of one or more encoded Data Transmissions either sent or received by the Parties to this TPE.

1.8 Individual

Individual person(s) whose claims for payment of services may be eligible to be paid under the terms of the applicable federal, State or local governmental program for which DMH processes or administers claims. It is acknowledged and agreed between the Parties that claim payments for purposes of this TPE will be made directly to Providers on behalf of such Individuals.

1.9 Lost or Indecipherable Transmission

A Data Transmission which is never received by or cannot be processed to completion by the intended recipient whether DMH, Trading Partner, and/or Agents in the format or composition received because it is garbled or incomplete, regardless of how or why the message was rendered incomplete.

1.10 Provider

Hospitals, clinics or persons duly licensed or certified to provide mental health services to Covered Individuals of Los Angeles County.

1.11 Source Documents

Documents containing Data which is or may be required as part of Data Transmission with respect to a claim for payment for mental health services rendered to an eligible Individual. Examples of Data contained within a specific Source Document include, without limitation, the following: Individual's name and identification number, claim number, diagnosis code for the service rendered, dates of service, procedure code, applicable charges, the Provider's name and/or Provider number.

1.12 Submitter ID Number

A Data Universal Numbering System identifier assigned by Dun & Bradstreet (D&B) to the Trading Partner or Agent for the purpose of identifying the Trading Partner for Data Transmissions is required by DMH for claiming transmissions.

1.13 System

The equipment and software necessary for a successful electronic Data Transmission.

1.14 Trading Partner

A Provider who has entered into this with DMH in order to satisfy all or part of its obligations under a Legal Entity or Network Provider Agreement by means of EDI.

2. OBLIGATIONS OF THE PARTIES

2.1 Mutual Obligations

In addition to the obligations of the respective Parties which are set forth elsewhere in this TPE, the mutual obligations of DMH, the Trading Partner and/or the Trading Partner's Agents collectively referred to as "the Parties" shall include, but not be limited to, the following:

(a) Accuracy of EDI Transmission

The Parties shall take reasonable care to ensure that Data and Data Transmissions are timely, complete, accurate and secure, and shall take reasonable precautions to prevent unauthorized access to the System of the other Party, the Data Transmission itself or the contents of an Envelope which is transmitted either to or from either Party pursuant to this TPE. Parties shall also take reasonable care to ensure accurate and unduplicated transmissions are sent to recipients and shall notify the recipient of all erroneous duplicated transmissions timely. Parties shall also take necessary actions to correct and void any and all invalid transmissions.

(b) Re-transmission of Indecipherable Transmissions

Where there is evidence that a Data Transmission is Lost or Indecipherable, the sending Party shall make best efforts to trace and re-transmit the original Data Transmission in a manner which allows it to be processed by the intended receiving Party as soon as practicable.

(c) Cost of Equipment

Each Party shall, at its own expense, obtain and maintain its own System and shall update its System as recommended by the manufacturer/owner/licensor of said System. Furthermore, each Party shall pay its own costs for any and all charges related to Data Transmission under this TPE and specifically including, without limitation, charges for System equipment, software and services, charges for maintaining an electronic mailbox, connect time, terminals, connections, telephones, modems, and any applicable minimum use charges. Each Party shall also be responsible for any and all expenses it incurs for translating, formatting, or sending and receiving communications over the electronic network to the electronic mailbox, if any, of the other Party.

(d) Back-up Files

Each Party shall maintain adequate back-up files and/or electronic tapes or other means sufficient to re-create a Data Transmission in the event that such re-creation becomes necessary for any purpose at any time. Such back-up files and/or tapes shall be subject to the terms of this exhibit to the same extent as the original Data Transmission.

(e) Format of Transmissions

Except as otherwise provided herein, each Party shall send and receive all Data Transmissions in the format designated by DMH to the Trading Partner.

(f) Testing

Each Party shall, prior to the initial Data Transmission and throughout the term of the underlying contract, test and cooperate with the other Party in the testing of the Systems of both Parties as DMH considers reasonably necessary to ensure

the accuracy, timeliness, completeness and confidentiality of each Data Transmission.

2.2 Trading Partner Obligations

In addition to the requirements of Section 2.1 and 4.1, the Trading Partner shall be specifically obligated as follows:

(a) To refrain from copying, reverse engineering, disclosing, publishing, distributing or altering any Data, Data Transmissions, DMH provided interfaces, or applications, or use of the same for any purpose other than that for which the Trading Partner was specifically given access and authorization by DMH;

(b) To refrain from obtaining Data, Data Transmission(s), access to DMH interfaces or solutions for any purpose other than access DMH expressly authorizes to said Trading Partner. Furthermore, in the event that the Trading Partner receives Data, Data Transmissions, or access other than expressly authorized by DMH, Trading Partner shall immediately cease use of said Data, Data Transmission(s), interface(s) or application(s), notify DMH and make arrangements to return Data or Data Transmission. Upon confirmation of receipt by DMH of said Data, Data Transmissions, Trading Partner shall immediately destroy Data and/or Data Transmission contained in such Data Transmission from its System, records, or network(s).

(c) To implement security measures to ensure the integrity and confidentiality of both DMH and the Trading Partner's data and/or records when the System is not in active use by the Trading Partner.

(d) To protect and maintain the confidentiality of the DMH issued Secure Identification Tokens of the Trading Partner or Agent at all times.

(e) To enforce encryption and secure authentication where appropriate, by utilizing complex passwords and/or by other mutually agreed upon means in order to ensure the transmission of the data is maintained secure during all data exchanges between Trading Partners and DMH.

(f) Prior to or upon execution of the underlying contract, provide DMH, in writing, all of the information requested in the Trading Partner Information section of the TPE online application. While the underlying contract is in effect, the Trading Partner shall notify DMH in writing no later than ten (10) business days of any material changes in the information originally provided by the Trading Partner in the TPE online application.

(g) To minimize the risk of data loss during transmissions, Trading Partners must notify DMH of any planned System changes at least 30 days prior to any change.

2.3 DMH Obligations

In addition to the obligations of DMH set forth herein, DMH shall be specifically obligated as follows:

(a) Availability of Data

DMH shall make available to the Trading Partner by electronic means, those types of Data and Data Transmissions to which the Trading Partner is entitled to receive by mutual agreement of the Parties or as provided by law.

(b) Notices Regarding Formats

DMH shall provide Trading Partner a listing of acceptable electronic data transmission formats and shall notify Trading Partner of changes to acceptable data transmissions in accordance with the timelines specified in the underlying contract.

3. AGENTS

The Trading Partner may use, in the performance of the underlying contract with DMH, various third parties as the Trading Partner's Agents in the electronic exchange of information as such the following will apply:

3.1 Responsibility of Agents

If the Trading Partner uses the services of an Agent in any capacity in order to receive, transmit, store or otherwise process Data or Data Transmissions or perform related activities, the Trading Partner shall be fully liable to DMH or for any acts, failures or omissions of the Agent in providing said services as though they were the Trading Partner's own acts, failures, or missions. Upon request by DMH, Trading Partners must also provide documentation demonstrating that all Agents have current and applicable Business Associate Agreements in order to represent said Trading Partner.

3.2 Notices Regarding Agents

Prior to the commencement of the Agent's services in the performance of the specified obligations in this TPE, the Trading Partner shall designate in the TPE online application, its specific Agents who are authorized to send and/or receive Data Transmissions in the performance of the aforementioned obligations on behalf of the Trading Partner. Except as provided otherwise in this TPE, the Trading Partner shall notify DMH of any material changes in the information contained in the TPE online application, no less than ten (10) days prior to the effective date of such changes. The information within the TPE application, when fully executed, shall be incorporated into this TPE by reference and shall be effective upon execution of the underlying contract, unless specified otherwise. The Trading Partner's designation of its Agent for purposes of this TPE is expressly subject to the approval of DMH, which will not be unreasonably withheld.

3.3 Express Warranties Regarding Agents

The Trading Partner expressly warrants that the Agent will make no changes in the Data content of any Data Transmissions or the contents of an Envelope, and further that such Agent will take all appropriate measures to maintain the timeliness, accuracy, confidentiality and completeness of each Data Transmission. Furthermore, the Trading Partner expressly warrants that its Agents will be advised of, and will comply in all respects with, the terms of this TPE.

3.4 Indemnification Regarding Agents

The Trading Partner shall indemnify, defend and hold harmless DMH from any and all claims, actions, damages, liabilities, costs and expenses, specifically including, without limitation, reasonable attorney's fees and costs resulting from the acts or omissions of the Trading Partner, its Agents, employees, subcontractors in the performance of the underlying contract; provided however, that DMH shall have the option, at its sole discretion, to employ attorneys selected by it to defend any such action, the costs and expenses of which shall be the responsibility of the Trading Partner. DMH for its part shall provide the Trading Partner with timely notice of the existence of such proceedings and such information, documents and other cooperation as reasonably necessary to assist the Trading Partner in establishing a defense to such action.

4. SECURITY

4.1 General Requirements

In addition to the requirements of Sections 2.1 and 2.2, the Trading Partner shall maintain adequate security procedures to prevent unauthorized access to Data, Data Transmissions, or the System of DMH. Trading Partner shall immediately notify DMH of any and all unauthorized attempts by any person or entity to obtain access to or otherwise tamper with the Data, Data Transmissions or the System of DMH.

(a) Notice of Unauthorized Disclosures

The Trading Partner will promptly notify DMH of any and all unlawful or unauthorized disclosures of Confidential Information that comes to its attention and will cooperate with DMH in the event any litigation arises concerning the unauthorized use, transfer or disclosure of Confidential Information.

ELECTRONIC TRADING PARTNER EXHIBIT

The Trading Partner acknowledges, agrees to and shall be bound by all the terms, provisions and conditions of the Trading Partner Exhibit

Agreed To:

Trading Partner Name (Legal Entity / Network Provider)
(Type or Print)

_____	_____
Authorized Personnel (Type or Print)	**Authorized Signature**
_____	_____
Title (Type or Print)	**Date**

Contractor shall complete, sign, and submit the TPE annually.

ATTESTATION REGARDING INFORMATION SECURITY REQUIREMENTS

In accordance with Paragraph 9.13 of the Contract, (CONTRACTOR PROTECTION OF ELECTRONIC COUNTY INFORMATION), Contractor must comply with Los Angeles County Board of Supervisors Policy No. 5.200 "Contractor Protection of Electronic County Information" security and privacy requirements.

_____ (hereafter "Contractor") acknowledges and certifies that safeguards are in place to protect electronically stored and/or transmitted personal information (PI); protected health information (PHI) and medical information (MI).

Contractor acknowledges it is the Contractor's responsibility to access the following link: https://dmh.lacounty.gov/contract-exhibits **annually and upon notification by DMH of updated Information Security Exhibits to complete, or update, the forms listed below:**

- Exhibit Q – Information Security and Privacy Requirements for Contracts
- Exhibit R – DMH Contractor's Compliance with Information Security Requirements
- Exhibit T – Electronic Data Transmission Trading Partner Exhibit (TPE)

Further, Contractor agrees to comply with the terms and conditions of the exhibits listed above, which are by this reference made a part of the Contract. Contractor understands that it is the Contractor's responsibility to access the link above, sign and submit the listed Information Security Exhibits requiring signatures via email to the Contract Administrator listed in Exhibit E (County's Administration).

Name of authorized official (Official Name)_____

Printed name

Signature of authorized official _____ Date _____