

SUBORDINATE CONTRACT NO. MA-042-22010466
FOR
UNARMED SECURITY GUARD SERVICES
WITH
AG COAST, INC. DBA CALIFORNIA PANTHER SECURITY

This Subordinate Contract Number MA-042-22010466 (“Contract”), is made and entered into this 1st day of July, 2020 (“Effective Date”) between AG Coast Inc., dba California Panther Security (“Contractor”), with a place of 5777 W. Century Blvd Ste. 1601, Los Angeles, CA 90045 and County of Orange, a political subdivision of the State of California (“County”), through its Health Care Agency with a place of business at 200 Santa Ana Blvd., Suite 650, Santa Ana, CA 92701-7506, which are sometimes referred to individually as “Party” or collectively as “Parties”.

ATTACHMENTS

This Contract is comprised of this document and the following Attachments, which are incorporated by reference herein

Attachment A – Post Orders (Various HCA Locations)
Attachment B – Compensation and Invoicing
Attachment C – Business Associate Contract
Attachment C-1 – Personal Information Privacy and Security Contract
Attachment D – Regional Cooperative Agreement (RCA) No. RCA-017-20010006

RECITALS

WHEREAS, on February 26, 2020, the County declared a Local Emergency, and the County’s Health Officer declared a Local Health Emergency in response to COVID-19 emergency and outbreak, as necessary for the preservation of public health and safety; and

WHEREAS, on March 4, 2020, Governor Gavin Newsom declared a State of Emergency in the State of California concerning the COVID-19 emergency and outbreak; and

WHEREAS, on March 12, 2020, Governor Gavin Newsom issued Executive Order N-25-20, ordering all California residents to heed any orders and guidance of State and local public health officials, including but not limited to imposition of social distancing measures, to control the spread of COVID-19; and

WHEREAS, on March 18, 2020, the President of the United States proclaimed a national emergency concerning the COVID-19 outbreak; and

WHEREAS, on March 22, 2020, the President of United States declared a major disaster exists in the State of California and ordered Federal assistant to supplement State and local recovery efforts in the areas affected by the COVID-19 pandemic; and

WHEREAS, the Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA) has issued the Public Assistance Program and Policy Guide, Version 4 (Guide) that provides guidance on the availability of federal funding to states and local governments during emergencies pursuant to Section 502 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act); and

WHEREAS, the Guide identifies the services/commodities described herein as an eligible cost during emergencies; and

WHEREAS, the County of Orange, County Procurement Office, issued a Regional Cooperative Agreement No. RCA-017-20010006 for Unarmed Security Guard Services, effective April 1, 2020 through March 31, 2025; and

WHEREAS, the County of Orange/Health Care Agency (HCA) desires to enter into a Contract with Contractor for Unarmed Security Guard Services; and

WHEREAS, Contractor agrees to provide services to County in accordance with the terms and conditions of RCA No. RCA-017-20010006 and Post Orders, attached hereto as Attachment A; and

WHEREAS, County agrees to pay Contractor based on the schedule of fees set forth in Compensation and Invoicing, attached hereto as Attachment B; and

NOW, THEREFORE, the Parties mutually agree as follows:

ARTICLES

1. **Scope of Contract:** This Contract specifies the terms and conditions by which County will procure goods (“Services”) from Contractor , as more fully detailed in Attachment A – Post Orders and Attachment D - RCA No. RCA-017-20010006.
2. **Term of Contract:** This Contract shall commence on September 30, 2021 through ~~December~~March 31, ~~2023~~2025, unless otherwise terminated by County.
3. **Compensation & Payment:** Contractor shall provide the Services as set forth in Attachment A – Post Orders at the fee specified in Attachment B – Compensation and Invoicing.
4. **Contractor Screening:** Throughout the term of this Contract, Contractor shall not be listed on any state or federal exclusionary rosters, listed below. County may screen Contractor on a monthly basis to ensure Contractor is not listed on the exclusionary rosters, listed below. If Contractor or its employee(s) are found to be included on any of the rosters indicated below, Contractor shall be deemed in default of its obligation under this Paragraph and shall constitute a cause for County to exercise its right to terminate this Contract immediately. County, in its sole discretion, may afford Contractor an opportunity to cure said default within a reasonable time.
 - a. United States Department of Health and Human Services, Office of Inspector General (OIG) List of Excluded Individuals & Entities (LEIE) (<http://exclusions.oig.hhs.gov>).

Address: ~~200 W. Santa Ana Blvd Suite 650~~
~~Santa Ana, CA 92701~~
Telephone: ~~(714) 834-5021~~
E-mail: adiaz@ochea.com

(Signature Page Follows)

SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties have executed this Amendment No. **23**. If Contractor is a corporation, Contractor shall provide two signatures as follows: 1) the first signature must be either the Chairman of the Board, the President, or any Vice President; 2) the second signature must be either the Secretary, an Assistant Secretary, the Chief Financial Officer, or any Assistant Treasurer. In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution or by-laws demonstrating the legal authority of the signature to bind the company.

Contractor: AG Coast Corporation

Mahmoud Galal
Print Name

President
Title

Signature

Date

Mohamed Galal
Print Name

Secretary
Title

Signature

Date

County of Orange, a political subdivision of the State of California
Purchasing Agent/Designee Authorized Signature:

Print Name

Deputy Purchasing Agent
Title

Signature

Date

APPROVED AS TO FORM
Office of the County Counsel
Orange County, California

Print Name

Deputy County Counsel
Title

Signature

Date

ATTACHMENT A-1**POST ORDERS**

HCA shall provide post orders detailing important contact information, duties, procedures and hours of operation to each location where Unarmed Security Guards are assigned. A copy of the Post Order must be given to Contractor and Unarmed Security Guard at each location for use by guard staff.

Contractor shall provide unarmed security services on the following HCA Locations in accordance with the requirements set forth in the RCA and in this Attachment A.

Locations:

1. 2228 Ritchey Street, Santa Ana, CA 92705
2. Bldg. 360- 8226 Marine Way, Irvine, CA 92618

<u>Building Manager Contact Information:</u> <u>Various</u>	<u>Facility Hours of Operation:</u> <u>24/7</u>
<u>Unarmed Security Guard Duties:</u>	
<ol style="list-style-type: none"> <u>1. Maintain workstation and regularly patrol and monitor the building (interior, if requested, and exterior) including the parking lot for any unusual or suspicious activities.</u> <u>2. Observe and report any unsafe, unacceptable behavior, or security problems to Department project manager.</u> <u>3. Check in with Department project manager upon arrival to inquire if there are any special situations/circumstances the unarmed security guard should be aware of.</u> <u>4. Escort any individuals from the premises upon direction from Department project manager. Make sure individuals do not leave children unaccompanied.</u> <u>5. Request the assistance of local law enforcement or sheriff (if available) if an individual becomes abusive or unmanageable.</u> <u>6. Record the date, time, caller, reason for page resulting in activity on the Daily Activity Report (DAR).</u> <u>7. Unarmed security guards are to not: carry batons, mace, or pepper spray while working on County Property.</u> <u>8. Unarmed security guard shall not wear headphones, listen to music, or read unauthorized materials while on duty.</u> <u>9. Unarmed security guard shall not conduct personal phone calls except in the event of an emergency.</u> <u>10. No personal visitors of the unarmed security guard allowed on work site.</u> <u>11. Do not use County equipment nor telephone except to perform assigned duties.</u> <u>12. Do not attempt to force or enforce a corrective action other than escort individuals from premise.</u> <u>13. Do not accept any gratuities, nor be under the influence of drugs or alcohol on duty.</u> <u>14. No fraternization with clients. This includes smoking with clients.</u> <u>15. Contact Supervisor at California Panther Security, if out sick or running late.</u> <u>16. To complete, sign and provide a written report of all incidents and occurrences to the Department project manager staff within twenty-four (24) hours of the incident.</u> <u>17. Assist employees in evacuating individuals from the building during emergencies and evacuation drills.</u> <u>18. Other related duties may be assigned by the site manager.</u> 	
<u>Emergency Notification Numbers:</u>	

<u>911 and/or onsite supervisor</u>	
<u>Emergency Procedures: (please attach additional sheets if necessary)</u> <u>Please see attached.</u>	
<u>Fire Alarm System Instructions:</u>	<u>Security System Operating Instructions:</u>
<u>Door Location/Lock & Unlock Instructions:</u>	<u>Gate Location/Lock & Unlock Instructions:</u>
<u>Special Instructions: (please attach additional sheets if necessary)</u>	

ATTACHMENT A**POST ORDERS**

~~HCA shall provide post orders detailing important contact information, duties, procedures and hours of operation to each location where Unarmed Security Guards are assigned. A copy of the Post Order must be given to Contractor and Unarmed Security Guard at each location for use by guard staff.~~

~~Contractor shall provide unarmed security services on the following HCA Locations in accordance with the requirements set forth in the RCA and in this Attachment A.~~

- ~~● **Location: Various Vaccination PODS**~~

Post Order

Building Manager Contact Information:- Various	Facility Hours of Operation:- 24/7
--	--

Unarmed Security Guard Duties:

- ~~1. Maintain work station and regularly patrol and monitor the building (interior and exterior) including the parking lot for any unusual or suspicious activities.~~
- ~~2. Observe and report any unsafe, unacceptable behavior, or security problems to Department project manager.~~
- ~~3. Check in with Department project manager upon arrival to inquire if there are any special situations/circumstances the unarmed security guard should be aware of.~~
- ~~4. Escort any individuals from the premises upon direction from Department project manager. Make sure individuals do not leave children unaccompanied.~~
- ~~5. Request the assistance of local law enforcement or sheriff (if available) if an individual becomes abusive or unmanageable.~~
- ~~6. Record the date, time, caller, reason for page resulting in activity on the Daily Activity Report (DAR).~~
- ~~7. Unarmed security guards are to not: carry batons, mace, or pepper spray while working on County Property.~~
- ~~8. Unarmed security guard shall not wear headphones, listen to music, or read unauthorized materials while on duty.~~
- ~~9. Unarmed security guard shall not conduct personal phone calls except in the event of an emergency.~~
- ~~10. No personal visitors of the unarmed security guard allowed on work site.~~
- ~~11. Do not use County equipment nor telephone except to perform assigned duties.~~

<p>12. Do not attempt to force or enforce a corrective action other than escort individuals from premise.</p> <p>13. Do not accept any gratuities, nor be under the influence of drugs or alcohol on duty.</p> <p>14. No fraternization with clients. This includes smoking with clients.</p> <p>15. Contact Supervisor at California Panther Security, if out sick or running late.</p> <p>16. To complete, sign and provide a written report of all incidents and occurrences to the Department project manager staff within twenty-four (24) hours of the incident.</p> <p>17. Assist employees in evacuating individuals from the building during emergencies and evacuation drills.</p> <p>18. Other related duties may be assign by the site manager.</p>	
<p>Emergency Notification Numbers:- 911 and/or onsite supervisor</p>	
<p>Emergency Procedures: (please attach additional sheets if necessary) Please see attached.</p>	
<p>Fire Alarm System Instructions:</p>	<p>Security System Operating Instructions:</p>
<p>Door Location/Lock & Unlock Instructions:</p>	<p>Gate Location/Lock & Unlock Instructions:</p>
<p>Special Instructions: (please attach additional sheets if necessary)</p>	

ATTACHMENT B-1**COMPENSATION AND INVOICING**

1. **Compensation:** This is a fixed price Contract not to exceed the amount of \$1,723,000 for the Term of Contract.

Contractor agrees to accept the specified compensation as set forth in this Contract as full payment for performing all services and furnishing all staffing and materials required, for any reasonably unforeseen difficulties which may arise or be encountered in the execution of the services until acceptance, for risks connected with the services, and for performance by Contractor of all its duties and obligations hereunder. Contractor shall only be compensated as set forth herein for work performed in accordance with Attachment A – Post Orders.

2. **Fees and Charges:** County will pay the following fees in accordance with the provisions of this Contract.

See RCA-017-20010006, Attachment B-Compensation and Pricing

3. **Price Increase/Decreases:** No price increases will be permitted during the first period of the Contract. County requires documented proof of cost increases on the Contract prior to any price adjustment. A minimum of 30-days advance notice in writing is required to secure such adjustment. No retroactive price adjustments will be considered. All price decreases will automatically be extended to the County of Orange. County may enforce, negotiate, or cancel escalating price contracts or take any other action it deems appropriate, as it sees fit. The net dollar amount of profit will remain firm during the period of the Contract. Adjustments increasing Contractor's profit will not be allowed.

4. **Firm Discount and Pricing Structure:** Contractor guarantees that prices quoted are equal to or less than prices quoted to any other local, State or Federal government entity for services of equal or lesser scope. Contractor agrees that no price increases shall be passed along to County during the term of this Contract not otherwise specified and provided for within this Contract.

5. **Contractor's Expense:** Contractor will be responsible for all costs related to photo copying, telephone communications and fax communications while on County sites during the performance of work and services under this Contract.

6. **Payment Terms – Payment in arrears:** Invoices are to be submitted to the user agency/department to the ship-to address, unless otherwise directed in this Contract. Contractor shall reference the Contract number on invoice. Payment shall be made in arrears within 30 days after receipt of an invoice in a format acceptable to the County of Orange and verified and approved by the agency/department and subject to routine processing requirements. The responsibility for providing an acceptable invoice rests with Contractor.

Billing shall cover services and/or goods not previously invoiced. Contractor shall reimburse the County of Orange for any monies paid to Contractor for goods or services not provided or when goods or services do not meet the Contract requirements.

Payments made by County shall not preclude the right of County from thereafter disputing any items or services involved or billed under this Contract and shall not be construed as acceptance of any part of the goods or services.

7. Taxpayer ID Number: Contractor shall include its taxpayer ID number on all invoices submitted to County for payment to ensure compliance with IRS requirements and to expedite payment processing.

8. Payment – Invoicing Instructions: Contractor will provide an invoice on Contractor's letterhead for goods delivered and/or services rendered. In the case of goods, Contractor will leave an invoice with each delivery. Each invoice will have a number and will include the following information:

- a. Contractor's name and address
- b. Contractor's remittance address
- c. Contractor's Taxpayer ID Number
- d. Name of County Agency/Department
- e. Delivery/service address
- f. Master Agreement MA-042-22010466
- g. Agency/Department's Account Number, if applicable
- h. Date of invoice
- i. Product/service description, quantity, and prices
- j. Sales tax, if applicable
- k. Freight/delivery charges, if applicable
- l. Total

The responsibility for providing acceptable invoices to County for payment rests with Contractor. Incomplete or incorrect invoices are not acceptable and shall be returned to Contractor.

Invoice and support documentation shall be forwarded to either the County's Account Payable physical address or electronic email address: hcaap@ochca.com

or

Orange County Health Care Agency
Accounts Payable
PO Box 689
Santa Ana, CA 92702

9. Payment (Electronic Funds Transfer)

County offers Contractor the option of receiving payment directly to its bank account via an Electronic Fund Transfer (EFT) process in lieu of a check payment. Payment made via EFT shall also receive an Electronic Remittance Advice with the payment details via e-mail. An e-mail address shall need to be provided to County via an EFT Authorization Form. Contractor may request a form from the agency/department representative listed in the Contract.

~~ATTACHMENT B~~

~~COMPENSATION AND INVOICING~~

~~1. **Compensation:** This is a fixed price Contract not to exceed the amount of \$199,000 for the Term of Contract.~~

~~Contractor agrees to accept the specified compensation as set forth in this Contract as full payment for performing all services and furnishing all staffing and materials required, for any reasonably unforeseen difficulties which may arise or be encountered in the execution of the services until~~

~~acceptance, for risks connected with the services, and for performance by Contractor of all its duties and obligations hereunder. Contractor shall only be compensated as set forth herein for work performed in accordance with Attachment A—Post Orders.~~

- ~~2. **Fees and Charges:** County will pay the following fees in accordance with the provisions of this Contract.~~

~~See RCA 017-20010006, Attachment B Compensation and Pricing~~

- ~~3. **Price Increase/Decreases:** No price increases will be permitted during the first period of the Contract. County requires documented proof of cost increases on the Contract prior to any price adjustment. A minimum of 30 days advance notice in writing is required to secure such adjustment. No retroactive price adjustments will be considered. All price decreases will automatically be extended to the County of Orange. County may enforce, negotiate, or cancel escalating price contracts or take any other action it deems appropriate, as it sees fit. The net dollar amount of profit will remain firm during the period of the Contract. Adjustments increasing Contractor's profit will not be allowed.~~
- ~~4. **Firm Discount and Pricing Structure:** Contractor guarantees that prices quoted are equal to or less than prices quoted to any other local, State or Federal government entity for services of equal or lesser scope. Contractor agrees that no price increases shall be passed along to County during the term of this Contract not otherwise specified and provided for within this Contract.~~
- ~~5. **Contractor's Expense:** Contractor will be responsible for all costs related to photo copying, telephone communications and fax communications while on County sites during the performance of work and services under this Contract.~~
- ~~6. **Payment Terms—Payment in advance:** Invoices are to be submitted to the user agency/department to the ship to address, unless otherwise directed in this Contract. Contractor shall reference the Contract number on invoice. Payment shall be made in advance within 30 days after receipt of an invoice in a format acceptable to the County of Orange and verified and approved by the agency/department and subject to routine processing requirements. The responsibility for providing an acceptable invoice rests with Contractor.~~

~~Billing shall cover services and/or goods not previously invoiced. Contractor shall reimburse the County of Orange for any monies paid to Contractor for goods or services not provided or when goods or services do not meet the Contract requirements.~~

~~Payments made by County shall not preclude the right of County from thereafter disputing any items or services involved or billed under this Contract and shall not be construed as acceptance of any part of the goods or services.~~

- ~~7. **Taxpayer ID Number:** Contractor shall include its taxpayer ID number on all invoices submitted to County for payment to ensure compliance with IRS requirements and to expedite payment processing.~~
- ~~8. **Payment Invoicing Instructions:** Contractor will provide an invoice on Contractor's letterhead for goods delivered and/or services rendered. In the case of goods, Contractor will leave an invoice with each delivery. Each invoice will have a number and will include the following information:~~
- ~~a. Contractor's name and address~~
 - ~~b. Contractor's remittance address~~
 - ~~c. Contractor's Taxpayer ID Number~~
 - ~~d. Name of County Agency/Department~~
 - ~~e. Delivery/service address~~
 - ~~f. Master Agreement MA 042-22010466~~
 - ~~g. Agency/Department's Account Number, if applicable~~
 - ~~h. Date of invoice~~
 - ~~i. Product/service description, quantity, and prices~~
 - ~~j. Sales tax, if applicable~~
 - ~~k. Freight/delivery charges, if applicable~~
 - ~~l. Total~~

~~The responsibility for providing acceptable invoices to County for payment rests with Contractor. Incomplete or incorrect invoices are not acceptable and shall be returned to Contractor.~~

~~Invoice and support documentation shall be forwarded to either the County's Account Payable physical address or electronic email address:~~

Orange County Health Care Agency Accounts Payable PO Box 689 Santa Ana, CA 92702	hcaaccountspayable@ochca.com
---	--

- ~~9. **Payment (Electronic Funds Transfer)**
 County offers Contractor the option of receiving payment directly to its bank account via an Electronic Fund Transfer (EFT) process in lieu of a check payment. Payment made via EFT shall also receive an Electronic Remittance Advice with the payment details via e-mail. An e-mail address shall need to be provided to County via an EFT Authorization Form. Contractor may request a form from the agency/department representative listed in the Contract.~~

ATTACHMENT C**BUSINESS ASSOCIATE CONTRACT****A. GENERAL PROVISIONS AND RECITALS**

1. The parties agree that the terms used, but not otherwise defined below in Paragraph B, shall have the same meaning given to such terms under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (“the HITECH Act”), and their implementing regulations at 45 CFR Parts 160 and 164 (“the HIPAA regulations”) as they may exist now or be hereafter amended.

2. The parties agree that a business associate relationship under HIPAA, the HITECH Act, and the HIPAA regulations between the CONTRACTOR and COUNTY arises to the extent that CONTRACTOR performs, or delegates to subcontractors to perform, functions or activities on behalf of COUNTY pursuant to, and as set forth in, the Agreement that are described in the definition of “Business Associate” in 45 CFR § 160.103.

3. The COUNTY wishes to disclose to CONTRACTOR certain information pursuant to the terms of the Agreement, some of which may constitute Protected Health Information (“PHI”), as defined below in Subparagraph B.10, to be used or disclosed in the course of providing services and activities pursuant to, and as set forth, in the Agreement.

4. The parties intend to protect the privacy and provide for the security of PHI that may be created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement in compliance with the applicable standards, implementation specifications, and requirements of HIPAA, the HITECH Act, and the HIPAA regulations as they may exist now or be hereafter amended.

5. The parties understand and acknowledge that HIPAA, the HITECH Act, and the HIPAA regulations do not pre-empt any state statutes, rules, or regulations that are not otherwise pre-empted by other Federal law(s) and impose more stringent requirements with respect to privacy of PHI.

6. The parties understand that the HIPAA Privacy and Security rules, as defined below in Subparagraphs B.9 and B.14, apply to the CONTRACTOR in the same manner as they apply to a covered entity (COUNTY). CONTRACTOR agrees therefore to be in compliance at all times with the terms of this Business Associate Contract and the applicable standards, implementation specifications, and requirements of the Privacy and the Security rules, as they may exist now or be hereafter amended, with respect to PHI and electronic PHI created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement.

B. DEFINITIONS

1. “Administrative Safeguards” are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of CONTRACTOR’s workforce in relation to the protection of that information.

2. “Breach” means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

a. Breach excludes:

i. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of CONTRACTOR or COUNTY, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

ii. Any inadvertent disclosure by a person who is authorized to access PHI at CONTRACTOR to another person authorized to access PHI at the CONTRACTOR, or organized health care arrangement in which COUNTY participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

iii. A disclosure of PHI where CONTRACTOR or COUNTY has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

b. Except as provided in paragraph (a) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless CONTRACTOR demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used the PHI or to whom the disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and

iv. The extent to which the risk to the PHI has been mitigated.

3. “Data Aggregation” shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.

4. “Designated Record Set” shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.

5. “Disclosure” shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

6. “Health Care Operations” shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.

7. “Individual” shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

8. “Physical Safeguards” are physical measures, policies, and procedures to protect CONTRACTOR’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

9. “The HIPAA Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

10. “Protected Health Information” or “PHI” shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

11. “Required by Law” shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.103.

12. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his or her designee.

13. “Security Incident” means attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. “Security incident” does not include trivial incidents that occur on a daily basis, such as scans, “pings”, or unsuccessful attempts to penetrate computer networks or servers maintained by CONTRACTOR.

14. “The HIPAA Security Rule” shall mean the Security Standards for the Protection of electronic PHI at 45 CFR Part 160, Part 162, and Part 164, Subparts A and C.

15. “Subcontractor” shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

16. “Technical safeguards” means the technology and the policy and procedures for its use that

protect electronic PHI and control access to it.

17. “Unsecured PHI” or “PHI that is unsecured” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued on the HHS Web site.

18. “Use” shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

C. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE:

1. CONTRACTOR agrees not to use or further disclose PHI COUNTY discloses to CONTRACTOR other than as permitted or required by this Business Associate Contract or as required by law.

2. CONTRACTOR agrees to use appropriate safeguards, as provided for in this Business Associate Contract and the Agreement, to prevent use or disclosure of PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY other than as provided for by this Business Associate Contract.

3. CONTRACTOR agrees to comply with the HIPAA Security Rule at Subpart C of 45 CFR Part 164 with respect to electronic PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY.

4. CONTRACTOR agrees to mitigate, to the extent practicable, any harmful effect that is known to CONTRACTOR of a Use or Disclosure of PHI by CONTRACTOR in violation of the requirements of this Business Associate Contract.

5. CONTRACTOR agrees to report to COUNTY immediately any Use or Disclosure of PHI not provided for by this Business Associate Contract of which CONTRACTOR becomes aware. CONTRACTOR must report Breaches of Unsecured PHI in accordance with Paragraph E below and as required by 45 CFR § 164.410.

6. CONTRACTOR agrees to ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of CONTRACTOR agree to the same restrictions and conditions that apply through this Business Associate Contract to CONTRACTOR with respect to such information.

7. CONTRACTOR agrees to provide access, within fifteen (15) calendar days of receipt of a written request by COUNTY, to PHI in a Designated Record Set, to COUNTY or, as directed by COUNTY, to an Individual in order to meet the requirements under 45 CFR § 164.524. If CONTRACTOR maintains an Electronic Health Record with PHI, and an individual requests a copy of

such information in an electronic format, CONTRACTOR shall provide such information in an electronic format.

8. CONTRACTOR agrees to make any amendment(s) to PHI in a Designated Record Set that COUNTY directs or agrees to pursuant to 45 CFR § 164.526 at the request of COUNTY or an Individual, within thirty (30) calendar days of receipt of said request by COUNTY. CONTRACTOR agrees to notify COUNTY in writing no later than ten (10) calendar days after said amendment is completed.

9. CONTRACTOR agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by CONTRACTOR on behalf of, COUNTY available to COUNTY and the Secretary in a time and manner as determined by COUNTY or as designated by the Secretary for purposes of the Secretary determining COUNTY'S compliance with the HIPAA Privacy Rule.

10. CONTRACTOR agrees to document any Disclosures of PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY, and to make information related to such Disclosures available as would be required for COUNTY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.

11. CONTRACTOR agrees to provide COUNTY or an Individual, as directed by COUNTY, in a time and manner to be determined by COUNTY, that information collected in accordance with the Agreement, in order to permit COUNTY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.

12. CONTRACTOR agrees that to the extent CONTRACTOR carries out COUNTY'S obligation under the HIPAA Privacy and/or Security rules CONTRACTOR will comply with the requirements of 45 CFR Part 164 that apply to COUNTY in the performance of such obligation.

13. If CONTRACTOR receives Social Security data from COUNTY provided to COUNTY by a state agency, upon request by COUNTY, CONTRACTOR shall provide COUNTY with a list of all employees, subcontractors and agents who have access to the Social Security data, including employees, agents, subcontractors and agents of its subcontractors.

14. CONTRACTOR will notify COUNTY if CONTRACTOR is named as a defendant in a criminal proceeding for a violation of HIPAA. COUNTY may terminate the Agreement, if CONTRACTOR is found guilty of a criminal violation in connection with HIPAA. COUNTY may terminate the Agreement, if a finding or stipulation that CONTRACTOR has violated any standard or requirement of the privacy or security provisions of HIPAA, or other security or privacy laws are made in any administrative or civil proceeding in which CONTRACTOR is a party or has been joined. COUNTY

will consider the nature and seriousness of the violation in deciding whether or not to terminate the Agreement.

15 CONTRACTOR shall make itself and any subcontractors, employees or agents assisting CONTRACTOR in the performance of its obligations under the Agreement, available to COUNTY at no cost to COUNTY to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against COUNTY, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by CONTRACTOR, except where CONTRACTOR or its subcontractor, employee or agent is a named adverse party.

16. The Parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Business Associate Contract may be required to provide for procedures to ensure compliance with such developments. The Parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon COUNTY's request, CONTRACTOR agrees to promptly enter into negotiations with COUNTY concerning an amendment to this Business Associate Contract embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations or other applicable laws. COUNTY may terminate the Agreement upon thirty (30) days written notice in the event:

- a. CONTRACTOR does not promptly enter into negotiations to amend this Business Associate Contract when requested by COUNTY pursuant to this Paragraph C; or
- b. CONTRACTOR does not enter into an amendment providing assurances regarding the safeguarding of PHI that COUNTY deems are necessary to satisfy the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations.

17. CONTRACTOR shall work with COUNTY upon notification by CONTRACTOR to COUNTY of a Breach to properly determine if any Breach exclusions exist as defined in Subparagraph B.2.a above.

D. SECURITY RULE

1. CONTRACTOR shall comply with the requirements of 45 CFR § 164.306 and establish and maintain appropriate Administrative, Physical and Technical Safeguards in accordance with 45 CFR § 164.308, § 164.310, and § 164.312, with respect to electronic PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY. CONTRACTOR shall develop and maintain a written information privacy and security program that includes Administrative, Physical, and Technical Safeguards appropriate to the size and complexity of CONTRACTOR's operations and the nature and scope of its activities.

2. CONTRACTOR shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR Part 164, Subpart C, in compliance with 45 CFR § 164.316. CONTRACTOR will provide COUNTY with its current and updated policies upon request.

3. CONTRACTOR shall ensure the continuous security of all computerized data systems containing electronic PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY. CONTRACTOR shall protect paper documents containing PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY. These steps shall include, at a minimum:

- a. Complying with all of the data system security precautions listed under Paragraphs E, below;
- b. Achieving and maintaining compliance with the HIPAA Security Rule, as necessary in conducting operations on behalf of COUNTY;
- c. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies;

4. CONTRACTOR shall ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of CONTRACTOR agree through a contract with CONTRACTOR to the same restrictions and requirements contained in this Paragraph D of this Business Associate Contract.

5. CONTRACTOR shall report to COUNTY immediately any Security Incident of which it becomes aware. CONTRACTOR shall report Breaches of Unsecured PHI in accordance with Paragraph E below and as required by 45 CFR § 164.410.

6. CONTRACTOR shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this paragraph and for communicating on security matters with COUNTY.

//

//

E. DATA SECURITY REQUIREMENTS

1. Personal Controls

a. Employee Training. All workforce members who assist in the performance of functions or activities on behalf of COUNTY in connection with Agreement, or access or disclose PHI COUNTY

discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY, must complete information privacy and security training, at least annually, at CONTRACTOR's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following the termination of Agreement.

b. Employee Discipline. Appropriate sanctions must be applied against workforce members who fail to comply with any provisions of CONTRACTOR's privacy policies and procedures, including termination of employment where appropriate.

c. Confidentiality Statement. All persons that will be working with PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to such PHI. The statement must be renewed annually. The CONTRACTOR shall retain each person's written confidentiality statement for COUNTY inspection for a period of six (6) years following the termination of the Agreement.

d. Background Check. Before a member of the workforce may access PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The CONTRACTOR shall retain each workforce member's background check documentation for a period of three (3) years.

2. Technical Security Controls

a. Workstation/Laptop encryption. All workstations and laptops that store PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY either directly or temporarily must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the COUNTY.

b. Server Security. Servers containing unencrypted PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

c. Minimum Necessary. Only the minimum necessary amount of PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY required to perform necessary business functions may be copied, downloaded, or exported.

d. Removable media devices. All electronic files that contain PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Such PHI shall not be considered “removed from the premises” if it is only being transported from one of CONTRACTOR’s locations to another of CONTRACTOR’s locations.

e. Antivirus software. All workstations, laptops and other systems that process and/or store PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must have installed and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

f. Patch Management. All workstations, laptops and other systems that process and/or store PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release. Applications and systems that cannot be patched due to operational reasons must have compensatory controls implemented to minimize risk, where possible.

g. User IDs and Password Controls. All users must be issued a unique user name for accessing PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)

- Non-alphanumeric characters (punctuation symbols)

h. Data Destruction. When no longer needed, all PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission by COUNTY.

i. System Timeout. The system providing access to PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

j. Warning Banners. All systems providing access to PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

k. System Logging. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY, or which alters such PHI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If such PHI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

l. Access Controls. The system providing access to PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must use role based access controls for all user authentications, enforcing the principle of least privilege.

m. Transmission encryption. All data transmissions of PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI in motion such as website access, file transfer, and E-Mail.

n. Intrusion Detection. All systems involved in accessing, holding, transporting, and protecting PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY that are accessible via the Internet must be protected by a

comprehensive intrusion detection and prevention solution.

3. Audit Controls

a. System Security Review. CONTRACTOR must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

b. Log Reviews. All systems processing and/or storing PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must have a routine procedure in place to review system logs for unauthorized access.

c. Change Control. All systems processing and/or storing PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. Business Continuity/Disaster Recovery Control

a. Emergency Mode Operation Plan. CONTRACTOR must establish a documented plan to enable continuation of critical business processes and protection of the security of PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

b. Data Backup Plan. CONTRACTOR must have established documented procedures to backup such PHI to maintain retrievable exact copies of the PHI. The plan must include a regular schedule for making backups, storing backup offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data. Business Continuity Plan (BCP) for contractor and COUNTY (e.g. the application owner) must merge with the DRP.

5. Paper Document Controls

a. Supervision of Data. PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that

information is not being observed by an employee authorized to access the information. Such PHI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

b. Escorting Visitors. Visitors to areas where PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY is contained shall be escorted and such PHI shall be kept out of sight while visitors are in the area.

c. Confidential Destruction. PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must be disposed of through confidential means, such as cross cut shredding and pulverizing.

d. Removal of Data. PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must not be removed from the premises of the CONTRACTOR except with express written permission of COUNTY.

e. Faxing. Faxes containing PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

f. Mailing. Mailings containing PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY shall be sealed and secured from damage or inappropriate viewing of PHI to the extent possible. Mailings which include 500 or more individually identifiable records containing PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of COUNTY to use another method is obtained.

F. BREACH DISCOVERY AND NOTIFICATION

1. Following the discovery of a Breach of Unsecured PHI , CONTRACTOR shall notify COUNTY of such Breach, however both parties agree to a delay in the notification if so advised by a law enforcement official pursuant to 45 CFR § 164.412.

a. A Breach shall be treated as discovered by CONTRACTOR as of the first day on which such Breach is known to CONTRACTOR or, by exercising reasonable diligence, would have been known to CONTRACTOR.

b. CONTRACTOR shall be deemed to have knowledge of a Breach, if the Breach is

known, or by exercising reasonable diligence would have known, to any person who is an employee, officer, or other agent of CONTRACTOR, as determined by federal common law of agency.

2. CONTRACTOR shall provide the notification of the Breach immediately to the COUNTY Privacy Officer.

a. CONTRACTOR'S notification may be oral, but shall be followed by written notification within 24 hours of the oral notification.

3. CONTRACTOR'S notification shall include, to the extent possible:

a. The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by CONTRACTOR to have been, accessed, acquired, used, or disclosed during the Breach;

b. Any other information that COUNTY is required to include in the notification to Individual under 45 CFR §164.404 (c) at the time CONTRACTOR is required to notify COUNTY or promptly thereafter as this information becomes available, even after the regulatory sixty (60) day period set forth in 45 CFR § 164.410 (b) has elapsed, including:

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

(2) A description of the types of Unsecured PHI 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);

(3) Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

(4) A brief description of what CONTRACTOR is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any future Breaches; and

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

4. COUNTY may require CONTRACTOR to provide notice to the Individual as required in 45 CFR § 164.404, if it is reasonable to do so under the circumstances, at the sole discretion of the COUNTY.

5. In the event that CONTRACTOR is responsible for a Breach of Unsecured PHI in violation of the HIPAA Privacy Rule, CONTRACTOR shall have the burden of demonstrating that CONTRACTOR made all notifications to COUNTY consistent with this Paragraph F and as required by the Breach notification regulations, or, in the alternative, that the acquisition, access, use, or disclosure of PHI did not

constitute a Breach.

6. CONTRACTOR shall maintain documentation of all required notifications of a Breach or its risk assessment under 45 CFR § 164.402 to demonstrate that a Breach did not occur.

7. CONTRACTOR shall provide to COUNTY all specific and pertinent information about the Breach, including the information listed in Section E.3.b.(1)-(5) above, if not yet provided, to permit COUNTY to meet its notification obligations under Subpart D of 45 CFR Part 164 as soon as practicable, but in no event later than fifteen (15) calendar days after CONTRACTOR's initial report of the Breach to COUNTY pursuant to Subparagraph F.2 above.

8. CONTRACTOR shall continue to provide all additional pertinent information about the Breach to COUNTY as it may become available, in reporting increments of five (5) business days after the last report to COUNTY. CONTRACTOR shall also respond in good faith to any reasonable requests for further information, or follow-up information after report to COUNTY, when such request is made by COUNTY.

9. If the Breach is the fault of CONTRACTOR, CONTRACTOR shall bear all expense or other costs associated with the Breach and shall reimburse COUNTY for all expenses COUNTY incurs in addressing the Breach and consequences thereof, including costs of investigation, notification, remediation, documentation or other costs associated with addressing the Breach.

G. PERMITTED USES AND DISCLOSURES BY CONTRACTOR

1. CONTRACTOR may use or further disclose PHI COUNTY discloses to CONTRACTOR as necessary to perform functions, activities, or services for, or on behalf of, COUNTY as specified in the Agreement, provided that such use or Disclosure would not violate the HIPAA Privacy Rule if done by COUNTY except for the specific Uses and Disclosures set forth below.

a. CONTRACTOR may use PHI COUNTY discloses to CONTRACTOR, if necessary, for the proper management and administration of CONTRACTOR.

b. CONTRACTOR may disclose PHI COUNTY discloses to CONTRACTOR for the proper management and administration of CONTRACTOR or to carry out the legal responsibilities of CONTRACTOR, if:

i. The Disclosure is required by law; or

ii. CONTRACTOR obtains reasonable assurances from the person to whom the PHI is disclosed 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 person and the person immediately notifies CONTRACTOR

of any instance of which it is aware in which the confidentiality of the information has been breached.

c. CONTRACTOR may use or further disclose PHI COUNTY discloses to CONTRACTOR to provide Data Aggregation services relating to the Health Care Operations of CONTRACTOR.

2. CONTRACTOR may use PHI COUNTY discloses to CONTRACTOR, if necessary, to carry out legal responsibilities of CONTRACTOR.

3. CONTRACTOR may use and disclose PHI COUNTY discloses to CONTRACTOR consistent with the minimum necessary policies and procedures of COUNTY.

4. CONTRACTOR may use or disclose PHI COUNTY discloses to CONTRACTOR as required by law.

H. PROHIBITED USES AND DISCLOSURES

1. CONTRACTOR shall not disclose PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 USC § 17935(a) and 45 CFR § 164.522(a).

2. CONTRACTOR shall not directly or indirectly receive remuneration in exchange for PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY, except with the prior written consent of COUNTY and as permitted by 42 USC § 17935(d)(2).

I. OBLIGATIONS OF COUNTY

1. COUNTY shall notify CONTRACTOR of any limitation(s) in COUNTY'S notice of privacy practices in accordance with 45 CFR § 164.520, to the extent that such limitation may affect CONTRACTOR'S Use or Disclosure of PHI.

2. COUNTY shall notify CONTRACTOR of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect CONTRACTOR'S Use or Disclosure of PHI.

3. COUNTY shall notify CONTRACTOR of any restriction to the Use or Disclosure of PHI that COUNTY has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect CONTRACTOR'S Use or Disclosure of PHI.

4. COUNTY shall not request CONTRACTOR to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by COUNTY.

J. BUSINESS ASSOCIATE TERMINATION

1. Upon COUNTY’S knowledge of a material breach or violation by CONTRACTOR of the requirements of this Business Associate Contract, COUNTY shall:

a. Provide an opportunity for CONTRACTOR to cure the material breach or end the violation within thirty (30) business days; or

b. Immediately terminate the Agreement, if CONTRACTOR is unwilling or unable to cure the material breach or end the violation within (30) days, provided termination of the Agreement is feasible.

2. Upon termination of the Agreement, CONTRACTOR shall either destroy or return to COUNTY all PHI CONTRACTOR received from COUNTY or CONTRACTOR created, maintained, or received on behalf of COUNTY in conformity with the HIPAA Privacy Rule.

a. This provision shall apply to all PHI that is in the possession of Subcontractors or agents of CONTRACTOR.

b. CONTRACTOR shall retain no copies of the PHI.

c. In the event that CONTRACTOR determines that returning or destroying the PHI is not feasible, CONTRACTOR shall provide to COUNTY notification of the conditions that make return or destruction infeasible. Upon determination by COUNTY that return or destruction of PHI is infeasible, CONTRACTOR shall extend the protections of this Business Associate Contract to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for as long as CONTRACTOR maintains such PHI.

3. The obligations of this Business Associate Contract shall survive the termination of the Agreement.

//

//

//

//

Attachment C-1

Personal Information Privacy and Security Contract

Any reference to statutory, regulatory, or contractual language herein shall be to such language as in effect or as amended.

A. DEFINITIONS

1. "Breach" shall have the meaning given to such term under the IEA and CMPPA. It shall include a "PII loss" as that term is defined in the CMPPA.

2. "Breach of the security of the system" shall have the meaning given to such term under the California Information Practices Act, Civil Code § 1798.29(d).

3. "CMPPA Agreement" means the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (CHHS).

4. "DHCS PI" shall mean Personal Information, as defined below, accessed in a database maintained by the COUNTY or California Department of Health Care Services (DHCS), received by CONTRACTOR from the COUNTY or DHCS or acquired or created by CONTRACTOR in connection with performing the functions, activities and services specified in the Agreement on behalf of the COUNTY.

5. "IEA" shall mean the Information Exchange Agreement currently in effect between the Social Security Administration (SSA) and DHCS.

6. "Notice-triggering Personal Information" shall mean the personal information identified in Civil Code section 1798.29(e) whose unauthorized access may trigger notification requirements under Civil Code § 1709.29. For purposes of this provision, identity shall include, but not be limited to, name, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, a photograph or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper or any other medium.

7. "Personally Identifiable Information" (PII) shall have the meaning given to such term in the IEA and CMPPA.

8. "Personal Information" (PI) shall have the meaning given to such term in California Civil

Code§ 1798.3(a).

9. "Required by law" means a mandate contained in law that compels an entity to make a use or disclosure of PI or PII that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

10. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PI, or confidential data utilized in complying with this Agreement; or interference with system operations in an information system that processes, maintains or stores PI.

B. TERMS OF AGREEMENT

1. Permitted Uses and Disclosures of DHCS PI and PII by CONTRACTOR. Except as otherwise indicated in this Exhibit, CONTRACTOR may use or disclose DHCS PI only to perform functions, activities, or services for or on behalf of the COUNTY pursuant to the terms of the Agreement provided that such use or disclosure would not violate the California Information Practices Act (CIPA) if done by the COUNTY.

2. Responsibilities of CONTRACTOR

CONTRACTOR agrees:

a) Nondisclosure. Not to use or disclose DHCS PI or PII other than as permitted or required by this Personal Information Privacy and Security Contract or as required by applicable state and federal law.

b) Safeguards. To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of DHCS PI and PII, to protect against anticipated threats or hazards to the security or integrity of DHCS PI and PII, and to prevent use or disclosure of DHCS PI or PII other than as provided for by this Personal Information Privacy and Security Contract. CONTRACTOR shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of CONTRACTOR's operations and the nature and scope of its activities, which incorporate the requirements of Paragraph (c), below. CONTRACTOR will provide COUNTY with its current policies upon request.

c) Security. CONTRACTOR shall ensure the continuous security of all computerized data systems containing DHCS PI and PII. CONTRACTOR shall protect paper documents containing DHCS PI and PII. These steps shall include, at a minimum:

i. Complying with all of the data system security precautions listed in Paragraph E of the Business Associate Contract, Attachment C to the Agreement. ; and

ii. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III-Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies.

iii. If the data obtained by CONTRACTOR from COUNTY includes PII, CONTRACTOR shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement (IEA). The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. CONTRACTOR also agrees to ensure that any of CONTRACTOR's agents or subcontractors, to whom CONTRACTOR provides DHCS PII agree to the same requirements for privacy and security safeguards for confidential data that apply to CONTRACTOR with respect to such information.

d) Mitigation of Harmful Effects. To mitigate, to the extent practicable, any harmful effect that is known to CONTRACTOR of a use or disclosure of DHCS PI or PII by CONTRACTOR or its subcontractors in violation of this Personal Information Privacy and Security Contract.

e) CONTRACTOR's Agents and Subcontractors. To impose the same restrictions and conditions set forth in this Personal Information and Security Contract on any subcontractors or other agents with whom CONTRACTOR subcontracts any activities under the Agreement that involve the disclosure of DHCS PI or PII to such subcontractors or other agents.

f) Availability of Information. To make DHCS PI and PII available to the DHCS and/or COUNTY for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of DHCS PI and PII. If CONTRACTOR receives DHCS PII, upon request by COUNTY and/or DHCS, CONTRACTOR shall provide COUNTY and/or DHCS with a list of all employees, contractors and agents who have access to DHCS PII, including employees, contractors and agents of its subcontractors and agents.

g) Cooperation with COUNTY. With respect to DHCS PI, to cooperate with and assist the COUNTY to the extent necessary to ensure the DHCS's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of DHCS PI, correction of errors in DHCS PI, production of DHCS PI, disclosure of a security breach involving DHCS PI and notice of such breach to the affected individual(s).

h) Breaches and Security Incidents. During the term of the Agreement, CONTRACTOR agrees to implement reasonable systems for the discovery of any breach of unsecured DHCS PI and PII or security incident. CONTRACTOR agrees to give notification of any breach of unsecured DHCS PI and PII or security incident in accordance with Paragraph F, of the Business Associate Contract, Attachment C to the Agreement.

i) Designation of Individual Responsible for Security. CONTRACTOR shall designate an individual, (e.g., Security Officer), to oversee its data security program who shall be responsible for carrying out the requirements of this Personal Information Privacy and Security Contract and for communicating on security matters with the COUNTY.

ATTACHMENT D

REGIONAL COOPERATIVE AGREEMENT (RCA) NO. RCA-017-20010006