CONTRACT NO. MA-042-16011691

FOR

ELECTRONIC NURSE CASE MANAGEMENT SYSTEM

BETWEEN

THE COUNTY OF ORANGE
HEALTH CARE AGENCY

AND

PERSIMMONY INTERNATIONAL, INC.

TABLE OF CONTENTS **Page No.**

CONTRACT NO. MA-042-16011691

FOR

ELECTRONIC NURSE CASE MANAGEMENT SYSTEM

This Contract Number MA-042-16011691 (hereinafter "Contract"), is made and entered into this 1st day of November, 2016 or upon execution of all necessary signatures between Persimmony International, Inc. (hereinafter "Contractor"), a Nevada Corporation, with a place of business at 33 endless Vista, Aliso Viejo, CA 92656 and the County of Orange (hereinafter "County"), a political subdivision of the State of California, with a place of business at 200 Santa Ana Blvd., Ste. 650, Santa Ana, CA 92701-7506, which are sometimes individually referred to as "party", or collectively referred to as "parties".

RECITALS

WHEREAS, County desires to enter into a Contract for Electronic Nurse Case Management System; and

WHEREAS, Contractor agrees to render all the necessary skills, knowledge, material and labor to perform the services; and

WHEREAS, County has authorized the Purchasing Agent or designee to enter into Contract with Contractor for obtaining said services; and

NOW, THEREFORE, the parties mutually agree as follows:

ARTICLES

GENERAL TERMS AND CONDITIONS

A. Governing Law and Venue: This Contract has been negotiated and executed in the State of California and shall be governed by and construed under the laws of the State of California. In the event of any legal action to enforce or interpret this Contract, the sole and exclusive venue shall be a court of competent jurisdiction located in Orange County, California, and the parties hereto agree to and do hereby submit to the jurisdiction of such court, notwithstanding Code of Civil Procedure Section 394. Furthermore, the parties specifically agree to waive any and all rights to request that an action be transferred for trial to another county.

B. Entire Contract: This Contract, when accepted by Contractor either in writing or by commencement of performance hereunder, contains the entire Contract between the parties with respect to the matters herein and there are no restrictions, promises, warranties or undertakings other than those set forth herein or referred to herein. No exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing. Electronic acceptance of any additional terms, conditions or supplemental Contracts by any County employee or agent, including but not limited to installers of software, shall not be valid or binding on County unless accepted in writing by County's Purchasing Agent or designee, hereinafter "Purchasing Agent".

C. Amendments: No alteration or variation of the terms of this Contract shall be valid unless made in writing and signed by the parties; no oral understanding or agreement not incorporated herein shall be binding on either of the parties; and no exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing.

D. Taxes: Unless otherwise provided herein or by law, price quoted does not include California state sales or use tax.

E. **Delivery:** Time of delivery of services is of the essence in this Contract. County reserves the right to refuse any services and to cancel all or any part of the services that do not conform to the prescribed Scope of Work. Delivery shall not be deemed to be complete until all services have actually been received and accepted in writing by County.

F. **Acceptance/Payment:** County shall pay Contractor in accordance with the terms specified in Compensation and Invoicing (Attachment B) and Cost Table (Attachment C), upon County's acceptance of satisfactory services performed.

G. **Warranty:** Contractor warrants to County that the software shall be provided in accordance with the documentation and specifications provided in the Scope of Work, Attachment A. County's sole and exclusive remedy for any breach of the warranty described in this Section shall be at the discretion of Contractor, the repair or replacement of the software, or a prorated refund of the fees paid for by County if Contractor is not able to repair or replace the software. Except for express warranties set forth in this Contract, Contractor expressly disclaims all other warranties, whether express, implied, statutory or otherwise, with respect to the services or program provided to the County under this Contract, including without limitation all implied warranties of merchantability, quality, fitness for a particular purpose, and warranties arising from a course of dealing, usage, or trade practice.

H. **Patent/Copyright Materials/Proprietary Infringement:** Unless otherwise expressly provided in this Contract, Contractor shall be solely responsible for clearing the right to use any patented or copyrighted materials in the performance of this Contract. Contractor warrants that any software as modified through services provided hereunder will not infringe upon or violate any patent, copyright, trademark, trade secret, or any other proprietary right (Intellectual Property Right) of any third party. Contractor shall have the right, at its option, to (i) replace or modify the software so that it is functionally equivalent and non-infringing, (ii) obtain a license for County to continue using the software, or (iii) return the fees paid for any unused portion of the services by County therefore.

I. **Assignment or Subcontracting:** The terms, covenants, and conditions contained herein shall apply to and bind the heirs, successors, executors, administrators and assigns of the parties. Furthermore, neither the performance of this Contract nor any portion thereof may be assigned or sub-contracted by Contractor without the express written consent of County. Any attempt by Contractor to assign or subcontract the performance or any portion thereof of this Contract without the express written consent of County shall be invalid and shall constitute a breach of this Contract. Notwithstanding the above, Contractor uses third party independent contractors to assist with performing the services, and consent is hereby given with respect to the use of the independent contractors by Contractor.

J. **Non-Discrimination:** In the performance of this Contract, Contractor agrees that it shall comply with the requirements of Section 1735 of the California Labor Code and not engage nor permit any subcontractors to engage in discrimination in employment of persons because of the race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status of such persons. Contractor acknowledges that a violation of this provision shall subject Contractor to all the penalties imposed for a violation of Section 1720 et seq. of the California Labor Code.

K. **Termination:** In addition to any other remedies or rights it may have by law, County has the right to terminate this Contract without penalty immediately with cause or after thirty (30) days' written notice without cause, unless otherwise specified. Contractor has the right to terminate this Contract without penalty immediately with cause or after ninety (90) days' written notice without cause, unless otherwise specified. Cause shall be defined as any breach of this Contract, or any

misrepresentation or fraud on the part of either party. Exercise by a party of its right to terminate the Contract shall relieve the other of all further obligations.

L. **Consent to Breach Not Waiver:** No term or provision of this Contract shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of, a breach by the other, whether express or implied, shall not constitute consent to, waiver of, or excuse for any other different or subsequent breach.

M. **Remedies Not Exclusive:** The remedies for breach set forth in this Contract are cumulative as to one another and as to any other provided by law, rather than exclusive; and the expression of certain remedies in this Contract does not preclude resort by either party to any other remedies provided by law.

N. **Independent Contractor:** Contractor shall be considered an independent contractor and neither Contractor, its employees, nor anyone working under Contractor shall be considered an agent or an employee of County. Neither Contractor, its employees, nor anyone working under Contractor, shall qualify for workers' compensation or other fringe benefits of any kind through County.

O. **Performance:** Contractor shall perform all work under this Contract, taking necessary steps and precautions to perform the work to County's satisfaction. Contractor shall be responsible for the professional quality, technical assurance, timely completion and coordination of all documentation and other services furnished by Contractor under this Contract. Contractor shall perform all work diligently, carefully, and in a good and workman-like manner; shall furnish all labor, supervision, machinery, equipment, materials, and supplies necessary, therefore; shall at its sole expense obtain and maintain all permits and licenses required by public authorities, including those of County required in its governmental capacity, in connection with performance of the work; and, if permitted to subcontract, shall be fully responsible for all work performed by subcontractors.

P. **Insurance Provisions:** Prior to the provision of services under this Contract, Contractor agrees to purchase all required insurance at Contractor's expense and to deposit with County Certificates of Insurance, including all endorsements required herein, necessary to satisfy County that the insurance provisions of this Contract have been complied with and to keep such insurance coverage and the certificates therefore on deposit with County during the entire term of this Contract. In addition, all subcontractors performing work on behalf of Contractor pursuant to this Contract shall obtain insurance subject to the same terms and conditions as set forth herein for Contractor.

All self-insured retentions (SIRs) and deductibles shall be clearly stated on the Certificate of Insurance. If no SIRs or deductibles apply, indicate this on the Certificate of Insurance with a zero (0) by the appropriate line of coverage. Any self-insured retention (SIR) or deductible in an amount in excess of $25,000 ($5,000 for automobile liability), shall specifically be approved by the County Executive Office (CEO)/Office of Risk Management. If Contractor fails to maintain insurance acceptable to County for the full term of this Contract, County may terminate this Contract.

QUALIFIED INSURER

The policy or policies of insurance must be issued by an insurer licensed to do business in the State of California (California Admitted Carrier) or have a minimum rating be A- (Secure A.M. Best's Rating) and VIII (Financial Size Category as determined by the most current edition of the **Best's Key Rating Guide/Property-Casualty/United States or ambest.com**.

If the insurance carrier is not a non-admitted carrier in the State of California and does not have an A.M. Best rating of A-/VIII, the County CEO/Office of Risk Management retains the right to approve

or reject a carrier after a review of the company's performance and financial ratings.The policy or policies of insurance maintained by Contractor shall provide the minimum limits and coverage as set forth below:

Coverage	Minimum Limits
Commercial General Liability	$1,000,000 per occurrence $2,000,000 aggregate
Automobile Liability including coverage	$1,000,000 per occurrence for owned, non-owned and hired vehicles
Workers' Compensation	Statutory
Employers' Liability Insurance	$1,000,000 per occurrence
Network Security & Privacy Liability	$1,000,000 per claims made
Technology Errors & Omissions	$1,000,000 per claims made $1,000,000 aggregate

Required Coverage Forms

The Commercial General Liability coverage shall be written on Insurance Services Office (ISO) form CG 00 01, or a substitute form providing liability coverage at least as broad. The Business Auto Liability coverage shall be written on ISO form CA 00 01, CA 00 05, CA 0012, CA 00 20, or a substitute form providing coverage at least as broad.

Required Endorsements

The Commercial General Liability policy shall contain the following endorsements, which shall accompany the Certificate of Insurance:

a. An Additional Insured endorsement using ISO form CG 2010 or CG 2033 or a form at least as broad naming County of Orange, its elected and appointed officials, officers, employees, agents as Additional Insureds.

b. A primary non-contributing endorsement evidencing that Contractor’s insurance is primary and any insurance or self-insurance maintained by County of Orange shall be excess and non-contributing.

The Network Security and Privacy Liability policy shall contain the following endorsements which shall accompany the Certificate of Insurance:

1. An Additional Insured endorsement naming the County of Orange, its elected and appointed officials, officers, agents and employees as Additional Insureds for its vicarious liability.

2. A primary and non-contributing endorsement evidencing that Contractor’s insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

All insurance policies required by this Contract shall waive all rights of subrogation against the County of Orange and members of the Board of Supervisors, its elected and appointed officials, officers, agents and employees when acting within the scope of their appointment or employment.

The Workers' Compensation policy shall contain a waiver of subrogation endorsement waiving all rights of subrogation against the County of Orange, and members of the Board of Supervisors, its elected and appointed officials, officers, agents and employees.

Contractor shall notify County in Writing within thirty (30) days of any policy cancellation and ten (10) days for non-payment of premium and provide a copy of the cancellation notice to County. Failure to provide written notice of cancellation may constitute a material breach of the Contract, upon which County may suspend or terminate this Contract.

If Contractor's, Technology Errors & Omissions and~~/or~~ Network Security & Privacy Liability are "Claims Made" policy(ies), Contractor shall agree to maintain coverage for two (2) years following the completion of the Contract.

The Commercial General Liability policy shall contain a severability of interests clause also known as a "separation of insureds" clause (standard in the ISO CG 0001 policy). Insurance certificates should be forwarded to the agency/department address listed on the solicitation.

If Contractor fails to provide the insurance certificates and endorsements within seven (7) days of notification by County Procurement Office/Purchasing or the agency/department purchasing division, award may be made to the next qualified vendor.

County expressly retains the right to require Contractor to increase or decrease insurance of any of the above insurance types throughout the term of this Contract. Any increase or decrease in insurance shall be as deemed by County of Orange Risk Manager as appropriate to adequately protect County.

County shall notify Contractor in writing of changes in the insurance requirements. If Contractor does not deposit copies of acceptable Certificates of Insurance and endorsements with County incorporating such changes within thirty (30) days of receipt of such notice, this Contract may be in breach without further notice to Contractor, and County shall be entitled to all legal remedies.

The procuring of such required policy or policies of insurance shall not be construed to limit Contractor's liability hereunder nor to fulfill the indemnification provisions and requirements of this Contract, nor act in any way to reduce the policy coverage and limits available from the insurer.

Q. **Bill and Liens:** Contractor shall pay promptly all indebtedness for labor, materials and equipment used in performance of the work. Contractor shall not permit any lien or charge to attach to the work or the premises, but if any does so attach, Contractor shall promptly procure its release and, in accordance with the requirements of paragraph "HH" below, indemnify, defend, and hold County harmless and be responsible for payment of all costs, damages, penalties and expenses related to or arising from or related thereto.

R. **Changes:** Contractor shall make no changes in the work or perform any additional work without County's specific written approval.

S. **Change of Ownership/Name, Litigation Status, Conflicts with County Interests:** Contractor agrees that if there is a change or transfer in ownership of Contractor's business prior to completion of this Contract, and the County agrees to an assignment of the Contract, the new owners shall be required under the terms of sale or other instruments of transfer to assume Contractor's duties and obligations contained in this Contract, and complete them to the satisfaction of the County.

County reserves the right to immediately terminate the Contract in the event the County determines that the assignee is not qualified or is otherwise unacceptable to the County for the provision of services under the Contract.

In addition, Contractor has the duty to notify the County in writing of any change in the Contractor's status with respect to name changes that do not require an assignment of the Contract. The Contractor is also obligated to notify the County in writing if the Contractor becomes a party to any litigation against the County, or a party to litigation that may reasonably affect the Contractor's performance under the Contract, as well as any potential conflicts of interest between Contractor and County that may arise prior to or during the period of Contract performance. While Contractor will be required to provide this information without prompting from the County any time there is a change in Contractor's name, conflict of interest or litigation status, Contractor must also provide an update to the County of its status in these areas whenever requested by the County.

The Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with County interests. In addition to the Contractor, this obligation shall apply to the Contractor's employees, agents, and subcontractors associated with the provision of goods and services provided under this Contract. The Contractor's efforts shall include, but not be limited to establishing rules and procedures preventing its employees, agents, and subcontractors from providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to influence or appear to influence County staff or elected officers in the performance of their duties."

T. **Force Majeure:** Contractor shall not be assessed with liquidated damages or unsatisfactory performance penalties during any delay beyond the time named for the performance of this Contract caused by any act of God, war, civil disorder, employment strike, or other cause beyond its reasonable control, provided Contractor gives written notice of the cause of the delay to County within thirty six (36) hours of the start of the delay and Contractor avails itself of any available remedies.

U. **Confidentiality:** Contractor agrees to maintain the confidentiality of all County and County-related records and information pursuant to all statutory laws relating to privacy and confidentiality that currently exist or exist at any time during the term of this Contract. All such records and information shall be considered confidential and kept confidential by Contractor and Contractor's staff, agents and employees.

V. **Compliance with Laws:** Contractor represents and warrants that services to be provided under this Contract shall fully comply, at Contractor's expense, with all standards, laws, statutes, restrictions, ordinances, requirements, and regulations (collectively "laws"), including, but not limited to those issued by County in its governmental capacity and all other laws applicable to the services at the time services are provided to and accepted by County.

W. **Freight FOB Destination:** Contractor assumes full responsibility for all transportation, transportation scheduling, packing, handling, insurance, and other services associated with delivery of all products deemed necessary under this Contract.

X. **Pricing:** The Contract amount shall include full compensation for providing all services as specified herein or when applicable, in the Scope of Work attached to this Contract, and no additional compensation shall be allowed therefor, unless otherwise provided for in this Contract.

Y. Intentionally left blank

Z **Terms and Conditions:** Contractor acknowledges that it has read and agrees to all terms and conditions included in this Contract.

AA. **Headings:** The various headings and numbers herein, the grouping of provisions of this Contract into separate clauses and paragraphs, and the organization hereof are for the purpose of convenience only and shall not limit or otherwise affect the meaning hereof.

BB. **Severability:** If any term, covenant, condition or provision of this Contract is held by a court of competent jurisdiction to be invalid, void or unenforceable, the remainder of the provisions hereof shall remain in full force and effect and shall in no way be affected, impaired or invalidated thereby.

CC. **Calendar Days:** Any reference to the word "day" or "days" herein shall mean calendar day or calendar days, respectively, unless otherwise expressly provided.

DD. **Attorneys Fees:** In any action or proceeding to enforce or interpret any provision of this Contract, or where any provision hereof is validly asserted as a defense, each party shall bear its own attorney's fees, costs and expenses.

EE. **Interpretation:** This Contract has been negotiated at arm's length and between persons sophisticated and knowledgeable in the matters dealt with in this Contract. In addition, each party has been represented by experienced and knowledgeable independent legal counsel of its own choosing, or has knowingly declined to seek such counsel despite being encouraged and given the opportunity to do so. Each party further acknowledges that it has not been influenced to any extent whatsoever in executing this Contract by any other party hereto or by any person representing either or both of them. Accordingly, any rule of law (including California Civil Code Section 1654) or legal decision that would require interpretation of any ambiguities in this Contract against the party that has drafted it is not applicable and is waived. The provisions of this Contract shall be interpreted in a reasonable manner to effect the purpose of the parties and this Contract.

FF. **Authority:** The parties to this Contract represent and warrant that this Contract has been duly authorized and executed and constitutes the legally binding obligation, enforceable in accordance with its terms.

GG. **Employee Eligibility Verification:** Contractor warrants that it fully complies with all federal and state statutes and regulations regarding the employment of aliens and others and that all its employees performing work under this Contract meet the citizenship or alien status requirement set forth in federal statutes and regulations. Contractor shall obtain, from all employees performing work hereunder, all verification and other documentation of employment eligibility status required by federal or state statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, 8 U.S.C. §1324 et seq., as they currently exist and as they may be hereafter amended. Contractor shall retain all such documentation for all covered employees for the period prescribed by the law.

HH. **Indemnification:** Contractor agrees to indemnify, defend with counsel approved in writing by County, with such approval not unreasonably withheld by County, and hold County, its elected and appointed officials, officers, employees, agents and those special districts and agencies for which County's Board of Supervisors acts as the governing Board ("County Indemnitees") harmless from any claims, demands or liability of any kind or nature, including but not limited to personal injury, property damage, or Intellectual Property Rights infringement arising from the services, products or other performance provided by Contractor pursuant to this Contract. If judgment is entered against Contractor and County by a court of competent jurisdiction because of the concurrent active negligence of County or County Indemnitees, Contractor and County agree that liability shall be apportioned as determined by the court. Neither party shall request a jury apportionment.

County shall indemnify, defend, and hold Contractor, its officers, employees, agents harmless from and against all liability, loss, expense, or claims for injury damages arising out of the performance of this Contract, but only in proportion to and to the extent such liability, loss, expense, or claims for injury or damages are caused by or result from the negligent or intentional acts or omissions of County, its officers, employees or agents.

Neither termination of this Contract nor completion of the acts to be performed under this Contract shall release any party from its obligation to indemnify as to claims or cause of action asserted.

II. Limitation of Liability: NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, CONTRACTOR'S LIABILITIES UNDER THIS CONTRACT, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), WARRANTY OR OTHERWISE SHALL BE LIMITED TO DIRECT DAMAGES NOT TO EXCEED THE AMOUNTS ACTUALLY RECEIVED BY CONTRACTOR UNDER THIS CONTRACT IN THE 12 MONTHS PRIOR TO THE DATE OF THE ACTION GIVING RISE TO THE CLAIM. NOTWITHSTANDING THE FOREGOING, IF ANY CLAIM IS COVERED BY AN INSURANCE POLICY STATED IN SECTION P, ANY RECOVERY OF PROCEEDS UNDER SUCH POLICIES UP TO THE STATED POLICY AMOUNTS IN SECTION P SHALL BE PAID TO COUNTY TO EXTENT CONTRACTOR'S DAMAGES EXCEED THE FOREGONG LIMITATION OF LIABILITY. IN NO INSTANCE SHALL THE LIMITATION OF LIABILITY IMPAIR THE COUNTY'S ABILITY TO SEEK REMEDY FOR DAMAGES THROUGH THE CONTRACTOR'S INSURANCE CARRIER. CONTRACTOR SHALL NOT BE LIABLE FOR ANY (A) SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF PROFITS, ARISING FROM OR RELATED TO A BREACH OF THIS AGREEMENT OR ANY ORDER OR THE OPERATION OR USE OF THE SOFTWARE AND SERVICES, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; OR (B) CLAIMS MADE A SUBJECT OF A LEGAL PROCEEDING AGAINST CONTRACTOR MORE THAN TWO YEARS AFTER ANY SUCH CAUSE OF ACTION FIRST AROSE.

JJ. **Audits/Inspections:** Contractor agrees to permit the County's Auditor-Controller or the Auditor-Controller's authorized representative (including auditors from a private auditing company hired by County) access during normal working hours to all books, accounts, records, reports, files, financial records, supporting documentation, including payroll and accounts payable/receivable records, and other papers or property of Contractor for the purpose of auditing or inspecting any aspect of performance under this Contract. The inspection and/or audit shall be confined to those matters connected with the performance of the Contract including, but not limited to, the costs of administering the Contract. County shall provide reasonable notice of such an audit or inspection.

County reserves the right to audit and verify Contractor's Records before final payment is made. Contractor agrees to maintain such records for possible audit for a minimum of three (3) years after final payment, unless a longer period of records retention is stipulated under this Contract or by law. Contractor agrees to allow interviews of any employees, Contractor's independent contractors or others who might reasonably have information related to such records.

Should Contractor cease to exist as a legal entity, Contractor's records pertaining to this Contract shall be forwarded to the surviving entity in a merger or acquisition or, in the event of liquidation, to County's Project Manager.

ADDITIONAL TERMS AND CONDITIONS

1. **Scope of Contract:** This Contract, together with its Attachments and Exhibits attached hereto and incorporated herein by reference, specifies the contractual terms and conditions by which County shall procure and receive services from Contractor. The detailed Scope of Work (SOW) is fully set forth and incorporated herein as Attachment A.

2. **Term of Contract:** This Contract shall be in effect from ~~November 1, 2016 July 1~~ July 1, 2020 through ~~June 30, 2019 June 30, 2020~~ June 30, 2021, non-renewable ~~for two (2) one (1) additional one (1) year periods upon agreement of both parties.~~ County does not have to give reason if it decides not to renew. Contract shall be in effect for the time periods specified, unless this Contract is earlier terminated by the parties in accordance with paragraphs 5, 6, and 7.

3. **Precedence:** The Contract documents consist of this Contract, and its Attachments and Exhibits. In the event of a conflict between the Contract documents, the order of precedence shall be the provisions of the main body of this Contract, i.e., those provisions set forth in the recitals and articles of this Contract, the Attachments and then the Exhibits.

4. **Pricing Structure:** Contractor agrees that no price/fee increases shall be passed along to County during the term of this Contract. Contractor may discount said prices anytime during the term of the Contract.

5. **Fiscal Appropriations – Subject to:** This Contract is subject to and contingent upon applicable budgetary appropriations being approved by the County of Orange Board of Supervisors for each fiscal year during the term of this Contract. If such appropriations are not approved, the Contract shall be terminated without penalty to County.

6. **Contingency of Funds:** Contractor acknowledges that funding or portions of funding for this Contract may also be contingent upon the receipt of funds from, and/or appropriation of funds by, the State of California to County. If such funding and/or appropriations are not forthcoming, or are otherwise limited, County may immediately terminate or modify this Contract without penalty.

7. **Termination**

   A. Termination – Default: If Contractor is in default of any of its obligations under this Contract and has not commenced cure within ten (10) days after receipt of a written notice of default from County and cured such default within time specified in the notice, County shall immediately be entitled to either commence resolution in accordance with this paragraph or to terminate this Contract by giving written notice to take effect immediately. Default shall include failure to carry out any of the requirements of this Contract, including, but not limited to persistently disregarding laws and or ordinances, not proceeding with the work as agreed to herein, or otherwise substantially violating any provision of this Contract. Upon termination of the Contract with Contractor, County may begin negotiations with a third-party contractor to provide services as specified in this Contract. The right of either Party to terminate this Contract hereunder shall not be affected in any way by its waiver of or failure to take action with response to any previous default.

   If County is in default of any of its obligations under this Contract and has not commenced cure within ten (10) days after receipt of a written notice of default from Contractor and cured such default within a reasonable time specified in the notice, Contractor shall immediately be entitled to either commence resolution in accordance with this paragraph or to terminate this Contract by giving written notice to take effect immediately. Default shall include failure to carry out any of the requirements of this Contract, including, but not limited to making payments to Contractor.

B. Termination – Orderly: After receipt of a termination notice from County, Contractor shall submit to County a termination claim, if applicable. Such claim shall be submitted promptly, but in no event later than sixty (60) days from the effective date of the termination, unless one or more extensions in writing are granted by County upon written request of Contractor. Upon termination County agrees to pay Contractor for all services performed prior to termination which meet the requirements of the Contract, provided, however, that such compensation plus previously paid compensation shall not exceed the total compensation set forth in the Contract. Upon termination or other expiration of this Contract, each party shall promptly return to the other party all papers, materials, and other properties of the other held by each for purposes of execution of the Contract. In addition, each party shall assist the other party in orderly termination of this Contract and the transfer of all aspects, tangible and intangible, as may be necessary for the orderly, non-disruptive business continuation of each party.

8. **County Project Manager:** County shall appoint a Project Manager to act as liaison with Contractor during the term of this Contract. County's Project Manager shall coordinate the activities of County staff assigned to work with Contractor.

9. **Contractor Project Manager:** Contractor shall appoint a Project Manager to direct Contractor's efforts in fulfilling Contractor's obligations under this Contract. Contractor's Project Manager shall be assigned to this project for the duration of this Contract and shall diligently pursue all work and services to meet the project time lines. County's Project Manager shall have the right to require the replacement of Contractor's Project Manager or any other Contractor's staff providing services under this Contract. County's Project Manager shall notify Contractor in writing of such action, and shall provide Contractor with information on the performance issues warranting the replacement. Contractor shall accomplish the replacement within three (3) business days after written notice by County's Project Manager. County's Project Manager shall notify the assigned Buyer to document the contract folder accordingly.

10. **Breach of Contract:** The failure of Contractor to comply with any of the provisions, covenants or conditions of this Contract shall be a material breach of this Contract. In such event County may, and in addition to any other remedies available at law, in equity, or otherwise specified in this Contract:

a. Afford Contractor written notice of the breach and ten (10) calendar days or such shorter time that may be specified in this Contract within which to cure the breach.

b. Discontinue payment to Contractor for and during the period in which Contractor is in breach.

c. Offset against any monies billed by Contractor but yet unpaid by County those monies disallowed pursuant to the above.

11. **County of Orange Child Support Enforcement:** In order to comply with the child support enforcement requirements of the County of Orange, within ten (10) days of notification of selection of award of Contract but prior to official award of Contract, the selected Contractor agrees to furnish to the contract administrator, the Purchasing Agent, or the agency/department deputy purchasing agent:

a. In the case of an individual contractor, his/her name, date of birth, social security number, and residence address.

b. In the case of a contractor doing business in a form other than as an individual, the name, date of birth, social security number, and residence address of each individual who owns an interest of ten (10) percent or more in the contracting entity.

c. A certification that Contractor has fully complied with all applicable federal and state reporting requirements regarding its employees.
d. A certification that Contractor has fully complied with all lawfully served Wage and Earnings Assignment Orders and Notices of Assignment and shall continue to so comply.

Failure of Contractor to timely submit the data and/or certifications required may result in the Contract being awarded to another contractor. In the event a Contract has been issued, failure of Contractor to comply with all federal, state, and local reporting requirements for child support enforcement or to comply with all lawfully served Wage and Earnings Assignment Orders and Notices of Assignment shall constitute a material breach of the Contract. Failure to cure such breach within sixty (60) calendar days of notice from County shall constitute grounds for termination of the Contract.

12. Conflict of Interest: Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of County. This obligation shall apply to Contractor; Contractor's employees, agents, and relatives; sub-tier Vendors; and third parties associated with accomplishing work and services hereunder. Contractor's efforts shall include, but not be limited to establishing precautions to prevent its employees or agents from making, receiving, providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to appear to influence individuals to act contrary to the best interests of County.

The County of Orange Board of Supervisors' policy prohibits its public employees from engaging in activities involving conflicts of interest. Contractor shall not, during the period of this Contract, employ any County employee for any purpose.

13. Contractor Bankruptcy/Insolvency: If Contractor should be adjudged bankrupt or should have a general assignment for the benefit of its creditors or if a receiver should be appointed on account of Contractor's insolvency, County may terminate this Contract.

14. Disputes – Contract: The parties shall deal in good faith and attempt to resolve potential disputes informally. If the dispute concerning a question of fact arising under the terms of this Contract is not disposed of in a reasonable period of time by Contractor and County's Project Manager, such matter shall be brought to the attention of the Purchasing Agent by way of the following process:

a. Contractor shall submit to the agency/department assigned buyer a written demand for a final decision regarding the disposition of any dispute between the parties arising under, related to, or involving this Contract, unless County, on its own initiative, has already rendered such a final decision.

b. Contractor's written demand shall be fully supported by factual information, and, if such demand involves a cost adjustment to the Contract, Contractor shall include with the demand a written statement signed by a senior official indicating that the demand is made in good faith, that the supporting data are accurate and complete, and that the amount requested accurately reflects the Contract adjustment for which Contractor believes County is liable.

Pending the final resolution of any dispute arising under, related to, or involving this Contract, Contractor agrees to diligently proceed with the performance of this Contract, including the provision of services. Contractor's failure to diligently proceed shall be considered a material breach of this Contract.

Any final decision of County shall be expressly identified as such, shall be in writing, and shall be signed by the Purchasing Agent. If County fails to render a decision within ninety (90) days after receipt of Contractor's demand, it shall be deemed a final decision adverse to Contractor's

contentions. County's final decision shall be conclusive and binding regarding the dispute unless Contractor commences action in a court of competent jurisdiction to contest such decision within ninety (90) days following the date of County's final decision or one (1) year following the accrual of the cause of action, whichever is later.

16. Contractor's Records: Contractor shall provide services and other relevant documents necessary to complete the services and fulfill the requirements as set forth in Attachment A, SOW. Contractor shall keep true and accurate accounts, records, books and data which shall correctly reflect the business transacted by Contractor in accordance with generally accepted accounting principles. These records shall be stored in Orange County for a period of three (3) years after final payment is received from County. Storage of records in another county shall require written approval from the assigned buyer. Alternatively, the records can be stored online.

17. News/Information Release: Contractor agrees that it shall not issue any news releases or upload County logos or other information onto any website in connection with either the award of this Contract or any subsequent amendment of or effort under this Contract without first obtaining review and written approval from County through County's Project Manager. All press releases, including graphic display information to be published in newspapers, magazines, etc., are to be administered only by County unless otherwise agreed to by both parties.

18. California Public Records Act: Contractor and County agree and acknowledge that all information and documents related to the award and performance of this Contract are subject to disclosure pursuant to the California Public Records Act, California Government Code Section 6250 *et seq.*

19. Gratuities: Contractor warrants that no gratuities, in the form of entertainment, gifts or otherwise, were offered or given by Contractor or any agent or representative of Contractor to any officer or employee of County with a view toward securing the Contract or securing favorable treatment with respect to any determinations concerning the performance of the Contract. For breach or violation of this warranty, County shall have the right to terminate the Contract, either in whole or in part, and any loss or damage sustained by County in procuring on the open market any goods or services which Contractor agreed to supply shall be borne and paid for by Contractor. The rights and remedies of County provided in the clause shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

20. Amendments – Changes/Extra Work: Contractor shall make no changes to this Contract without County's written consent. In the event that there are new or unforeseen requirements, County with Contractor's concurrence has the discretion to request official changes at any time without changing the intent of this Contract.

If County-initiated changes or changes in laws or government regulations affect price, Contractor's ability to deliver services, or the project schedule, Contractor shall give County written notice no later than seven (7) calendar days from the date the law or regulation went into effect or the date the change was proposed by County and Contractor was notified of the change. Such changes shall be agreed to in writing and incorporated into a Contract amendment. Said amendment shall be issued by County-assigned buyer, shall require the mutual consent of all parties, and may be subject to approval by the County Board of Supervisors.

21. Reports/Meetings: Contractor shall develop reports and any other relevant documents necessary to complete the services and requirements as set forth in this Contract. County's Project Manager and Contractor's Project Manager shall meet on reasonable notice to discuss Contractor's performance and progress under this Contract. If requested, Contractor's Project Manager and other project personnel shall attend all meetings. Contractor shall provide such information that is requested by County for the purpose of monitoring progress under this Contract.

22. **EDD Independent Contractor Reporting Requirements:** Effective January 1, 2001, the County of Orange is required to file federal Form 1099-Misc for services received from a "service provider" to whom County pays $600 or more or with whom County enters into a contract for $600 or more within a single calendar year. The purpose of this reporting requirement is to increase child support collection by helping to locate parents who are delinquent in their child support obligations.

The term "service provider" is defined in California Unemployment Insurance Code Section 1088.8, subparagraph B.2 as "an individual who is not an employee of the service recipient for California purposes and who received compensation or executes a contract for services performed for that service recipient within or without the state." The term is further defined by the California Employment Development Department to refer specifically to independent Vendors. An independent contractor is defined as "an individual who is not an employee of the ... government entity for California purposes and who receives compensation or executes a contract for services performed for that ... government entity either in or outside of California."

The reporting requirement does not apply to corporations, general partnerships, limited liability partnerships, and limited liability companies.

Additional information on this reporting requirement can be found at the California Employment Development Department web site located at www.edd.ca.gov/txicr.htm.

23. **Debarment:** Contractor shall certify that neither contractor nor its principles are presently debarred, proposed for debarment, declared ineligible or voluntarily excluded from participation in the transaction by any Federal department or agency. Where contractor as the recipient of federal funds, is unable to certify to any of the statements in the certification, contractor must include an explanation with their bid/proposal. Debarment, pending debarment, declared ineligibility or voluntary exclusion from participation by any Federal department or agency may result in the bid/proposal being deemed non-responsible.

24. **Lobbying:** On best information and belief, Contractor certifies no federal appropriated funds have been paid or shall be paid by, or on behalf of, Contractor to any person for influencing or attempting to influence an officer or employee of Congress; or an employee of a member of Congress in connection with the awarding of any federal contract, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

25. **Contractor Personnel-Drug Free Workplace:** Contractor hereby certifies compliance with Government Code Section 8355 in matters relating to providing a drug-free workplace. Contractor shall:

a. Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited and specifying actions to be taken against employees for violations, as required by Government Code Section 8355(a).

b. Establish a drug-free awareness program as required by Government Code Section 8355(b) to inform employees about all of the following:

   1. The dangers of drug abuse in the workplace.

   2. The organization's policy of maintaining a drug-free workplace.

   3. Any available counseling, rehabilitation and employee assistance programs.

4. Penalties that may be imposed upon employees for drug abuse violations.

c. Provide as required by Government Code Section 8355(c) that every employee who works under this Contract:

1. Shall receive a copy of the company's drug-free policy statement.

2. Shall agree to abide by the terms of the company's statement as a condition of employment under this Contract.

Failure to comply with these requirements may result in suspension of payments under the Contract or termination of the Contract or both, and Contractor may be ineligible for award of any future County contracts if County determines that any of the following has occurred:

a. Contractor has made false certification, or

b. Contractor violates the certification by failing to carry out the requirements as noted above.

26. **County's Ownership of Data**: County is and shall remain the owner of all of its confidential and/or proprietary information ("County Proprietary Information"). Such County Proprietary Information may include, but not by way of limitation, personal information, individually identifiable physical or mental health information and other data provided by County to Contractor for Contractor's performance of the services, or stored by County and/or persons under the County's control through any services provided hereunder ("Program Activity Data"). For purposed of this Contract, Program Activity Data shall be all information stored on the server hosted by Contractor for County, and all information clearly marked as such. Subject to the terms of this Contract, County hereby grants Contractor a limited, royalty-free, fully-paid up, nonexclusive license to process the Program Activity Data strictly as instructed by County or an authorized user and solely necessary to provide the services for County's benefit in the County for so long as County or any authorized user uploads or stores such Program Activity Data for processing by or on behalf of Contractor on Contractor's server.

27. **Contractor's Ownership of Software**: All patents, copyrights, circuit layouts, mask works, trade secrets, trademarks, and other proprietary rights in or related to the software are and will remain the exclusive property of Contractor, whether or not specifically recognized or perfected under the laws of the jurisdiction in which the software is used or licensed. Contractor may place copyright and/or proprietary notices, including hypertext links, within the software. County may not alter or remove these notices without Contractor's written permission. County may not have the right to, and agrees not to, attempt to restrain Contractor from using any skills or knowledge of a general nature acquired during the course of providing the services, including information publicly known or available or that could reasonably be acquired in similar work performed for another county. County will not take any action that jeopardizes Contractor's proprietary rights or acquire any right in the software or Contractor's confidential and proprietary information. Contractor will own rights in any copy, translation, modification, adaptation or derivation of the Software. Any custom programming, including all source and machine code and materials developed by Contractor, all intermediate and partial versions thereof, as well as all specifications, program materials, flow charts, notes, outlines and the like created in connection therewith shall be the sole and exclusive property of Contractor. At Contractor's request, County will obtain the execution of any instrument that may be appropriate to assign these rights to Contractor or to perfect these rights in Contractor's name. The software and Contractor's confidential and proprietary information will not be a work for hire.

28. **Software – Protection:** County agrees that all material appropriately marked or identified as confidential or proprietary, whether oral or written, and furnished hereunder are provided for

County's nonexclusive use for the purposes of this Contract only and shall be held in confidence. All confidential and proprietary data shall remain the property of Contractor. County agrees to take all reasonable steps to ensure that such data are not disclosed to others without prior written consent of Contractor. County shall ensure, prior to disposing of any media, that any licensed materials contained thereon have been erased or otherwise destroyed.

County agrees that it shall take appropriate action by instruction, agreement or otherwise with its employees or other persons permitted access to licensed programs and/or optional materials to satisfy its obligations under this Contract with respect to access, use, copying, modification and protection and security of licensed programs and optional materials during and after the term of this Contract.

29. **Software License:** Contractor hereby grants to County, and County accepts from Contractor, subject to the terms and conditions of this Contract, a non-exclusive, non-transferable, limited license to access and use the hosted software products list in this Contract, hereinafter referred to as "software products" during the term of this Contract.

30. **Software – Acceptance Testing:** Acceptance testing may be required as specified for all Contractor-supplied software as specified and listed in the Contract or order, including all software initially installed. Included in this clause are improved versions, including new releases, of this software, any such software which has been modified by Contractor to satisfy County requirements, and any substitute software provided by Contractor in lieu thereof, unless the Contract or order provides otherwise. The purpose of the acceptance test is to ensure that the software operates in substantial accord with Contractor's technical specifications and meets County's performance specifications.

31. **Software – Documentation:** Contractor agrees to provide to County, County-designated number of all manuals and other associated printed materials and updated versions thereof, which are necessary or useful to County in its use of the equipment or software provided hereunder. County shall designate the number of copies for production use and the number of copies for disaster recovery purposes and shall provide this information to Contractor. Alternatively, Contractor can provide an electronic copy or online access to such materials.

If additional copies of such documentation are required, Contractor shall provide such manuals at the request of County. The requesting agency/department shall be billed for the manuals and any associated costs thereto by invoice. Contractor agrees to provide such additional manuals at prices not in excess of charges made by Contractor to its best customers for similar publications.

32. **Software – Future Releases:** If improvement, upgraded, or enhancement versions of any software product under this Contract are developed by Contractor and are made available to other licensees, they shall be made available to County at County's option, provided such versions are operable on the same computer hardware configuration. The charge for such upgrading to the later version of the software shall be the difference between the price established by Contractor for the later version and the price specified herein or the then prevailing prices of the currently installed version.

33. **Compliance with County Information Technology Policies and Procedures: Policies and Procedures**

Contractor, its subcontractors, Contractor personnel, and all other agents and representatives of Contractor, shall at all times comply with and abide by all Information Technology (IT) policies and procedures of County that are provided or made available to Contractor that pertain to Contractor (and of which Contractor has been provided with advance notice) in connection with Contractor's performance under this Contract. Contractor shall cooperate with County in ensuring Contractor's compliance with the IT policies and procedures described in this Contract and as adopted and

made available by County from time-to-time, and any material violations or disregard of such IT policies or procedures shall, in addition to all other available rights and remedies of County, be cause for termination of this Contract. In addition to the foregoing, Contractor shall comply with the following:

Security and Policies

All performance under this Contract shall be in accordance with County's security requirements, policies, and procedures as set forth above and as modified, supplemented, or replaced by County from time to time, in its sole discretion, by providing Contractor with a written copy of such revised requirements, policies, or procedures reasonably in advance of the date that they are to be implemented and effective (collectively, the "Security Policies"). Contractor shall at all times use industry best practices and methods, and all applicable HIPAA privacy and security regulations with regard to the prevention, detection, and elimination, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County systems accessed in the performance of services in this Contract.

Information Access

County may require all Contractor personnel performing services under this Contract to execute a confidentiality and non-disclosure agreement concerning access protection and data security in the form provided by County. County shall authorize, and Contractor shall issue, any necessary information-access mechanisms, including access IDs and passwords, and Contractor shall take all commercially reasonable measures that comply with HIPAA security and privacy regulations to secure such mechanisms. Contractor shall provide each Contractor personnel with only such level of access as is required for such individual to perform his or her assigned tasks and functions. All County systems, and all data and software contained therein, including County data, County hardware and County software, used or accessed by Contractor: (a) shall be used and accessed by such Contractor solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of Contractor's obligations hereunder; and (b) shall not be used or accessed except as expressly permitted hereunder, or commercially exploited in any manner whatsoever, by Contractor, at any time.

Enhanced Security Procedures

County may, in its discretion, designate certain areas, facilities, or systems as requiring a higher level of security and access control. County shall notify Contractor in writing reasonably in advance of any such designation becoming effective. Any such notice shall set forth in reasonable detail the enhanced security or access-control procedures, measures, or requirements that Contractor shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Contractor shall fully comply with and abide by all such enhanced security and access measures and procedures as of such date,

Breach of Security

Any breach or violation by Contractor of any of the foregoing shall be deemed a material breach of a material obligation of Contractor under this Contract and may be deemed an incurable and material breach of a material obligation of Contractor under this Contract resulting in termination.

Conduct on County Premises

Contractor shall, at all times, comply with and abide by all reasonable policies and procedures of County (or that may be established thereby, from time to time) that pertain to conduct on County's premises, possession or distribution of contraband, or the access to, and security of, the Party's

real property or facilities, to the extent that Contractor has been provided with a copy of each such policy or procedure. Contractor shall exercise due care and diligence to prevent any injury to persons or damage to property while on the other Party's premises. The operation of vehicles by either Party's personnel on the other Party's property shall conform to posted and other applicable regulations and safe-driving practices. Vehicular accidents occurring on a Party's property and involving either Party's personnel shall be reported promptly to the appropriate Party's personnel. Each Party covenants that at all times during the Term, it, and its employees, agents, and subcontractors shall comply with, and take no action that results in the other Party being in violation of, any applicable federal, state, and local laws, ordinances, regulations, and rules. Each Party's personnel shall clearly identify themselves as the appropriate Party's personnel and not as employees of the other Party. When on the other Party's premises, each Party's personnel shall wear and clearly display identification badges or tags, as approved by the other Party.

Security Audits

Each Contract year, County may perform or have performed security reviews and testing based on an IT infrastructure review plan. Such testing shall ensure all pertinent County security standards as well as any customer agency requirements, such as federal tax requirements or HIPAA.

34. **Notices:** Any and all notices, requests, demands, and other communications contemplated, called for, permitted, or required to be given hereunder shall be in writing, except through the course of the parties' routine exchange of information and cooperation during the term of the work and services, and shall be deemed to have been duly given (a) upon actual in-person delivery, if delivery is by direct hand; or (b) upon delivery agreed to as the actual day of receipt or no greater than five (5) calendar days after being mailed (the date of mailing shall count as the first day), whichever occurs first by United States certified or registered mail, return receipt requested, postage prepaid, addressed to the appropriate party at the following address or such other address as the parties hereto may designate by written notice from time to time in the manner aforesaid:

For Contractor:	Name:	Persimmony International, Inc.
	Address:	33 Endless Vista, Aliso Viejo, CA 92656
	Attn:	Jud Slusser
	Phone:	949-422-8183
	Fax:	949-770-5550
	E-mail:	judson@persimmony.com
For County:	Name:	Orange Orange Health Care Agency/Purchasing
	Address:	200 W. Santa Ana Blvd., Suite 650 Santa Ana, CA 92701
	Attn:	Michel Lizotte
	Title:	Deputy Purchasing Agent
	Phone:	714-834-7674
	Fax:	714-834-2657
	E-mail:	mlizotte@ochca.com
CC:	Name:	Orange County Health Care Agency/PHN
	Address:	1725 W. 17th Street, Santa Ana CA 92701
	Attn:	Pat Orme
	Title:	Division Manager
	Phone:	714-934-7799
	E-mail:	porme@ochca.com

(SIGNATURE PAGE FOLLOWS)

CONTRACT SIGNATURE PAGE

IN WITNESS WHEREOF, the parties hereto have executed this Contract on the dates shown opposite their respective signatures below.

Contractor's name: PERSIMMONY INTERNATIONAL, INC.

Print Name	Title
Signature	Date
Print Name	Title
Signature	Date

If the company is a corporation two signatures are required: one signature by the Chairman of the Board, President, or any Vice President; and one signature by the Secretary, any Assistant Secretary, Chief Financial Officer or any Assistant Treasurer. If signed by one authorized individual only, a copy of the corporate resolution or by-laws whereby the board of directors has empowered said authorized individual to act on its behalf by his or her signature alone is required.

****

County of Orange, a political subdivision of the State of California

Christine Bavaro-Sutton	Procurement Manager
Print Name	Title
Signature	Date

****

Approved as to Form
Office of the County Counsel
County of Orange, California

County Counsel Deputy	Date

ATTACHMENT A
SCOPE OF WORK

A. Background

The Public Health Nursing Division (PHND) of the County of Orange Health Care Agency (HCA), collectively or individually referred to as "County", provides public health nursing services to individuals throughout the County. Public Health Nurses (PHNs) provide nursing services in the home and community, including Targeted Case Management (TCM), client advocacy, community resource information and assistance with accessing health care. Services are provided to all residents of the County who meet the criteria regardless of financial status. Nurses in PHND provide services in a variety of programs that target specific populations and/or health needs. Target populations include pregnant and parenting women, children, adult, and older adults with unmet health needs

The PHND provides over 35,000 public health nursing services to approximately 7,000 individuals annually, the majority being home visits. PHNs access the system remotely while in the field to document nursing encounters and to access community resources needed for patient referrals and health education. Depending on the type of visits, nurses may perform one (1) to four (4) visits per day.

B. Electronic Nurse Case Management System

1. Contractor's Electronic Nurse Case Management System (System) shall include, but not be limited to the following features: a) assessment, b) nursing notes, c) care plans, d) referral, e) reports, and f) TCM/MAA time survey.

2. Contractor's System shall have the capability to:

    a. Capture extensive demographic information; and document, view, and retrieve health-related information for clients, and family and community outcomes based on user role and permissions.

    b. Utilize software to submit TCM reimbursement billing directly to the state.

    c. Send client data to the Nurse Family Partnership (NFP) Program through a data feed to the National Service Office (NSO) NFP warehouse database.

    d. Access the System in the field utilizing mobile devices.

    e. Host up to one hundred (100) concurrent users.

3. Contractor shall achieve the following objectives:

    a. Implement a fully functioning, integrated, and compliant System that meets all system and functional requirements and capabilities referenced in this Contract no later than nine (9) months after Contract execution; except for any additional modules, which will be developed and implemented on an agreed upon scope, budget and implementation time table.

    b. Implement common agreed upon System customizations no later than nine (9) months after contract execution. Common agreed System customizations shall be defined as simple field additions and deletions; removal of fields; and changing the layout, color screens, input areas, and reports outside of standard canned reports; except for any additional modules, which will be developed and implemented on an agreed upon scope, budget and implementation time table.

    c. Complete migration and validation of County's client data from the current contracted electronic nurse case management system and NFP applications to Contractor's System nine (9) months after contract execution.

d. Complete training to key County staff no later than thirty (30) calendar days before go-live date.

4. Implementation, Initial Database Setup, Customization

a. Contractor shall develop and maintain all assessments and database field customizations for PHND programs that are incorporated into Contractor's System, whether TCM billable or not.

b. Contractor shall establish all assessments and database field customizations for the NFP Program, including, but not limited to those that are aligned with TCM billing. Contractor shall also provide the setup, configuration and maintenance of data collection and reporting of the NFP's NSO.

5. Data Migration and Conversion Requirements

a. Contractor shall be required to migrate specific basic demographic data from active and closed charts from County's current contracted electronic nurse case management system to Contractor's System, and to import corresponding case information as PDF files, and link to associated clients before Contractor's System go-live date. Contractor and County shall validate all migrated and mapped data.

b. Contractor shall migrate and map County's NFP data from NFP NSO's database warehouse to Contractor's System. Contractor and County shall validate all migrated and mapped NFP data.

6. Functional Requirements

a. Electronic documentation of PHN activities for multiple program protocols at the individual/family/community level.

b. Built-in safeguards for TCM audit protections.

c. Reporting of accurate and consistent TCM/MAA activities for monitoring and claiming.

d. Time surveys as required for TCM reimbursement.

e. Standardized statistical, management and outcome reports.

f. Direct data upload of required NFP metrics.

g. Electronic identification of family members for comprehensive case management.

h. Efficient access to the system for online charting in the field using a portable device.

i. Direct submission of required data and outcomes measures to the Orange County Children and Families Commission.

j. Online time survey for Targeted Case Management perpetual time survey.

7. License Usage Agreement

a. Contractor shall provide an estimated one hundred (100) end user licenses to County, as reflected in the licensure costs in Attachment C. Contractor payments shall be based on actual quarterly users.

b. Contractor shall provide up to to two hundred (200) end user Authenticated Referral Portal licenses to County.

c. County's end users shall only use the System for the purpose intended and authorized through this Attachment A. Unauthorized use shall include, but not be limited to (i) using the System to provide data processing services to any third-party persons, (ii) making copies of the System for distribution to third-parties, and (iii) reverse-engineering or decompiling the System for the purpose of designing or developing a System competitive with Contractor's System.

d. Contractor shall provide System support, database access, and all other services described herein to County's end users.

e. County shall be responsible for ensuring that only authorized end users access the System.

f. County shall be responsible for setting up new users and/or agencies (assigning passwords and creating shortcuts, etc.) and ongoing addition and/or deletion of new and/or existing users.

g. Contractor's license fees for County authorized users shall be inclusive for the following:

i) System Maintenance and Programming.

ii) Application Service Provider (ASP) Operations.

iii) User Subscription Licenses.

iv) System Customization Support.

v) Database Administration and Data Backups.

8. Data Ownership

Contractor shall establish and maintain a source code escrow, and County shall have access to the source code in the event of bankruptcy, dissolution, merger or other situation that may impact Contractor's ability to support Contractor's System.

All County data in the System shall remain the property of County. In the event the Contractor shall undergo a bankruptcy, dissolution, merger or other situation that may impact Contractor's ability to support Contractor's System, the contractor will export County data from the system in a useable data format approved by the County, as well as the data dictionary and all related information to facilitate continued use.

C. Technical Specifications

1. Internet Browsers

Contractor's System shall support the following Internet browsers, and maintain capabilty with all future releases of each browser.

a. Microsoft Internet Explorer 11 or later.

b. Google Chrome 50 or later.

c. All mobile platform browsers.

2. Mobility Requirements

   a. Be device agnostic, i.e., application performance shall be identical whether the end user is connecting from a desktop versus a tablet or mobile device.

   b. Menus and forms shall (i) scale to display appropriately on any device, regardless of screen resolution, aspect ratio, or orientation, (ii) be designed for optimal performance over slower or unreliable connections, e.g., VPN, satellite or burst wireless connections, Wi-Fi, or a tethered Internet connection, and (iii) be designed with touch interaction as the primary expected input method through the use of drop-down lists, on/off switches, and context-specific fields.

   c. Provide for alternate points of entry depending on the end user's device, e.g., mobile application for tablets, iPads and smart phones versus a full featured application for workstations and laptops.

3. Support Levels, Training, Documentation

   a. Support Levels

      i) Contractor shall provide First (1st) Tier Admin Support and Second (2nd) Tier End-User Support to County. Contractor shall provide comprehensive 1st Tier Admin Support to the County's Project Manager and their online tools so all End Users can receive one-on-one virtual training and support, plus 2nd Tier Admin Support for all authorized users if County's Project Manager(s) is unable to troubleshoot the Users Database problems.

      ii) 1st Tier Admin Support: support staff shall have unlimited access to Contractor's support staff and technical support team via phone, online or e-mail from 8:00 AM to 5:00 PM Pacific Standard Time (PST), Monday through Friday, excluding County holidays. Contractor shall respond in no more than four (4) hours of initial request. Emergency assistance shall be available seven days a week, twenty-four hours a day (24/7) for system failures or other emergency needs.

      iii) Contractor shall provide 2nd Tier End User Support to County. End Users shall first contact support staff for any questions, e.g., assessment inquiries, password re-sets, etc. If County's support staff is not able to answer or solve the authorized user's question , County's support staff shall contact Contractor support staff to help resolve the issue.

      iv) County's support staff shall have unlimited access to Contractor's technical support via phone, online or e-mail from 8:00 AM to 5:00 PM PST, Monday through Friday, excluding County holidays, in addition to contacting assigned Contractor's Project Manager(s).for questions about the System, e.g., adding new surveys, questionnaires, assessment, reports, and any other customization of the existing fields within the System.

      v) Contractor shall provide 24/7 access to all authorized users video training 24/7 that provides training "just in time" for any of the data entry screens in the system. The SHOW ME videos provide step-by-step demonstrations on how to enter data, run reports and setup new fields all at a pace that is comfortable for the user who can stop, repeat or get back to any portion of the video training at any time.

   b. Training

      i) Contractor's Project Manager(s) shall provide train-the-trainer training to County support staff and selected end users, and provide technical assistance and product training during the initial 'migration of data' phase and throughout the term of the Contract. Contractor shall train support staff to use the Software's "Shadow Tools" to share the user's screen so they can see things first-hand, and virtually apply hands-on technical assistance if needed, to safely and securely manage the user's computer and

applications. For remote access shadowing, Contractor's Software shall prompt the end user for acceptance before connecting.

ii) End Users: Contractor shall provide training to groups based on job function, logon group, and access rights. Training shall include all end user functionalities.

iii) Super Users: Contractor's training shall include, but not be limited to, End User level of instruction, ad hoc report generator, System aspects, problem solving, diagnosis, and problem resolution.

iv) Service Desk Staff: Contractor's training shall include, but not be limited to Super User level of instruction, and how to accurately triage and record issues for escalation to higher levels of support. Contractor shall grant Service Desk Staff rights within the System to create and maintain end user maintenance.

c. Video Training

Contractor shall provide videos that train users how to use the application, to add data and run reports. Contractor shall provide videos that train Super Users how to:

i) Use the application to add data and run reports.

ii) Use the Security Module to manage all aspects of users and security groups.

iii) Use the Setup Module to manage all settings in the applcaition.

4. System Performance and Uptime

Contractor shall ensure system availability is maintained at 99.8% uptime. Contractor shall ensure system performance is maintained at County approved established baseline levels at go-live.

5. Database Customization

a. Contractor and County shall mutually agree on customizations that Contractor shall provide at no additional cost to County, for all existing database functionalities in order to meet the needs of County, including customization of the following features below.

i) Modifications and customizations to the existing fields within the System.

ii) Unlimited number of assessments/surveys to assist end users to collect data on the clients they serve.

iii) Unlimited number of customized point-and-click or export reports from the System.

b. Additional fields not currently in the database shall require both parties to agree, in writing, upon the scope of those changes, to which Contractor shall provide County any estimate of time and fees that may be required to complete the requested customizations.

6. Report Requirements

a. Standard reports shall be accessible to end users. Contractor and County shall define and customize standard reports during System implementation and throughout the term of this Contract.

b. Ad-hoc reports shall be easily performed by super users.

c. Report data shall have the ability to be exported to common data formats such as Excel, MS Word, txt, and PDF formats.

d. Standard reports shall include demographics reports to include ethnicity, urgency, region, referral agency, enrollment data, relationship and city.

e. Case management reports shall include summary by client demographics, referrals, caseload, activity detail, follow-up evaluation, clients without assessments, assessment comparison, and screening score.

f. TCM reports shall include TCM activities by date, TCM encounters by case manager, encounter log, action plan summary, resources used, list of problems/needs by client, schedule list, schedule with time codes, TCM billing form, TCM upload, and billing errors.

g. GIS reports shall include zip code.

h. Growth chart reports shall include height, head, circumference and weight.

7. Hosting Server Accessibility, Uptime,

a. Contractor shall host System on its servers, and shall make access available to County authorized users twenty-four (24) hours, seven days a week (24/7). Server access may be unavailable in the event of routine maintenance, which Contractor shall schedule outside County business hours of 6:00 PM to 6:00 AM PST and on any weekend or County holiday; unexpected hardware failure; malicious attacks such as denial of service attacks; or other unforeseeable events which restrict outside access to the server.

b. Contractor shall not be responsible for user's computer hardware or software failures that restrict the users' ability to access the Software.

8. Contractor System Requirements

a. Contractor shall allow County to enter data into the System, query data, run reports, and analyze data. County and Contractor shall agree that completion of the tasks or milestones contained within the Project Plan satisfies Contractor's performance requirements of this Agreement.

b. Contractor shall be responsible for establishing System operations and maintenance procedures.

c. Contractor shall:

i) Distribute system upgrades and version replacements to County as defined under the license agreement; and applicable updated user and operational documentation and assist in its installation in the test environment and migration to production.

ii) Maintain the System program code to provide the functionality defined in project requirements

iii) Maintain compatibility and integration with any third party outcome reporting tools that have been implemented as part of the System. Should any of these packages be upgraded, HCA will notify the Contractor in advance, so that analysis and code changes can be implemented as quickly as possible.

iv) Maintain comprehensive change control procedures to control system versions and releases. Establish and maintain a release methodology except in the case of "break fix".

v) Create and maintain a test environment to fully test approved changes and enhancements to the System.

D. Implementation Requirements

1. Project Plan

a. Contractor shall host and configure the System for use by County according to the Project Plan

b. Before commencement of the project, Contractor shall provide County with a Project Plan and timeline, which shall be carried out by Contractor's Project Manager(s). Contractor shall provide a project organization chart describing the project charter, deliverables and milestones that will be in place for the duration of the project.

c. Contractor and County may mutually agree, in writing, to revise the Project Plan as needed.

d. Contractor shall develop monthly written project status reports summarizing key activities, reviewing the work plan for adherence and deviation from schedule, and identifying any issues and issue resolutions for the preceding reporting period. The monthly project status reports shall be presented by Contractor's Project Manager to County's Project Manager at monthly project management meetings. This report shall be the basis for advising HCA on project progress, and to identify issues with which HCA shall be made aware and work with Contractor to resolve. The reporting frequency shall increase if County or Contractor feel additional communication is needed or required.

e. Stress Test

Contractor shall conduct a stress test using realistic production volumes utilizing a predefined test script approved by HCA. Contractor shall work with HCA on correcting all problems that shall arise during this test.

f. User Acceptance Testing

Contractor shall conduct a User Acceptance Test to ensure that HCA users are able to successfully use the System and that all modified workflows, policies and procedures are consistent with the requirements. Contractor shall develop test scripts and data for this test, review the results and recommend initial system acceptance.

HCA users shall assist in the actual test and shall be responsible for final approval of User Acceptance Test recommendations. Contractor shall make any code corrections based on the results of the User Acceptance Test.

E. HIPAA Audit Requirements

1. Initial HIPAA Privacy and Security Audit

a. At no cost to County, Contractor shall have the initial HIPAA privacy and security audit performed as specified in the attached Security Requirements and Guidelines for Application Vendors (Attachment F) and Application Service Providers (Attachment F) by an external independent qualified third-party auditor. Prior to the implementation and activation (aka "go-live") of the System, and prior to any Contractor access of any PHL/PI protected data, Contractor shall provide County the results of the initial audit and evidence that any required corrective actions have been completed and implemented.

2. Recurring Annual Audits and Compliance

   a. At no cost to County, Contractor shall perform the HIPAA privacy and security audit as specified in the attached Security Requirements and Guidelines for Application Vendors (Attachment F) and Application Service Providers (Attachment F) on an annual basis, either by an external qualified third-party auditor or by qualified internal Contractor resources. Contractor shall maintain ongoing compliance with current applicable HIPAA privacy and security laws and regulations.

ATTACHMENT B
COMPENSATION AND INVOICING

I. COMPENSATION

This is a fixed price Contract not to exceed the amount of $~~1,035,956~~ ~~433,656~~ $447,524. County shall pay Contractor in accordance with the Cost Table in Attachment C.

Payment shall not be made on any costs incurred before Contractor has completed its HIPAA Audit requirements under Paragraph F(1) of Attachment A to County's satisfaction, and address any identified deficiencies not meeting HIPAA standards.

Contractor agrees to accept the specified compensation as full remuneration for performing all services and furnishing all staffing and materials called for; for any reasonably foreseen difficulties under the responsibility of Contractor which may arise or be encountered in the execution of the services until their acceptance; for risks connected with the services; and for performance by Contractor of all of its duties and obligations hereunder. The fixed price shall include the fee and all expenses related to the performance of work and services required to meet the tasks and deliverables in the SOW, set forth more fully in Attachment A. Contractor shall not be paid for any services or costs associated with Paragraph F of Attachment A.

II. PAYMENT TERMS

Contractor shall submit invoices to the address below. Payment of invoices shall be net thirty (30) days after the receipt of an acceptable invoice submitted in accordance with the terms set forth herein. The invoice shall be verified and approved by County's Project Manager, and shall be subject to routine processing requirements of County. Invoices shall not be paid if services have not been appropriately provided as determined by County's Project Manager.

Billing shall cover only those services not previously invoiced. Contractor shall reimburse County for any monies paid to Contractor for services not provided or when services do not meet the Contract requirements. Payment 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 services.

III. PAYMENT (ELECTRONIC FUNDS TRANSFER) - INVOICING INSTRUCTIONS

County offers Contractor the option of receiving payment directly to their 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 the agency/department representative listed in the Contract.

1. Invoices and all supporting documentation shall be submitted to County's Project Manager as follows:

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

2 Contractor shall provide a two-part invoice on Contractor's letterhead for services rendered. Each invoice shall have a number and shall include the following information:

a. Contractor's name and address, and remittance address (if different)
b. Contractor's Tax Identification Number or Employer's Identification Number
c. County agency name and service address
d. Master Agreement Number: MA-042-16011691
e. Description and date services provided
f. Amount of Payment Requested

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.

ATTACHMENT C
COST TABLE

Payment shall not be made on any costs incurred before Contractor has completed its HIPAA Audit Requirements under Paragraph F(1) of Attachment A to County's satisfaction.

User License Costs			
	Year 1	Year 2	Year 3
Electronic Case Management (ECM) Licensing Cost Per User	$2,600	$2,650	$2,754
Persimmony Referral Portal (PRP) Licensing Cost Per User	$90	$92	$93

Annual Costs			
ECM User Licenses (up to 100 users, payment based on actual number of quarterly users)	$173,333	$265,000	$275,400
PRP User Licenses (up to 200 users, payment based on actual number of quarterly users)	$12,000	$18,320	$18,654
Training/1st Tier Admin Support (NFP)	$2,333	$3,500	$3,500
Training/1st Tier Admin Support (TCM)	$2,333	$3,500	$3,500
Training/1st Tier Admin Support (Technical Assistance)	$2,333	$3,500	$3,500
Partner Discount	($12,750)	($12,000)	($7,000)
Sub-Total	$179,582	$281,820	$297,554

One-Time Costs			
Implementation/Initial Database Setup/Customization (PHND)	$25,000	$0	$0
Implementation/Initial Database Setup/Customization (NFP)	$15,000	$0	$0
Implementation/Initial Database Setup/Customization (Referral Module)	$20,000	$0	$0
Optional Data Migration & Optimization of Data (PHND)	$7,000	$0	$0
Optional Data Migration & Optimization of Data (NFP)	$10,000	$0	$0
Sub-Total	$77,000	$0	$0

Sub-Total Annual Costs			$758,956
Sub-Total One-time Costs			$77,000
Additional Services ($150/hour)*			$200,000
Grand Total Costs			$1,035,956

*County may request additional services from Contractor throughout the term of this agreement, which shall be reimbursed at $150/hour, up to the maximum obligation of $200,000. Contractor and County shall agree on the scope of work for additional services, and Contractor shall obtain County's approval in writing prior to beginning any additional services.

ATTACHMENT C-2

PRICING

User License Costs		
Description	Year 4	Year 5
Electronic Case Management (ECM) Licensing Cost per user	$2,836	$2,921
Annual Software and Support Costs		
ECM User Licenses (up to 100 users, payment based on actual quarterly users)	$283,600	$292,100
Referral Portal (site license up to 200 users)	$29,950	$29,950
Best Partner Discount	($10,000)	($7,000)
Training/1st Tier Admin Support (NFP) NFP support includes all issues related to the upload to NSO. One monthly up to 1 hour meeting is included. Support for issues related to the usage of NFP forms and reports	$4,400	$4,700
Training/1st Tier Admin Support (TCM) TCM support includes all issues related to the upload to and downloads from the State of California of TCM invoices. This also includes tasks related to TCM Reports and TCM QA. TCM Audit support is also included.	$4,400	$4,700
Training/1st Tier Admin Support (Technical Assistance) Technical Assistance includes all issues related to the generic functionality of ECM One monthly up to 1 hour meeting is included. Support for issues related to the usage generic forms and reports.	$4,400	$4,700
Scanners Licenses (3 included) 8 * $370	**$2,960**	**$2,960**
Segmented Servers/Appliances Licenses, Support	**$48,946**	**$50,414**
Sub-Total	$368,656	$382,524
*Additional Services ($175/hour)	$65,000	$65,000
Annual Costs	$433,656	$447,524
Grand Total Costs		$881,180

* County may request additional services* from Contractor throughout the term of this agreement, which shall be reimbursed at $175/hour. Contractor and County shall agree on the scope of work for additional services, and Contractor shall obtain County's approval in writing before beginning any additional services.

ATTACHMENT D

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 retains 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 that 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 that 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 E

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, Exhibit D 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, Exhibit D 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 F

County of Orange
Health Care Agency

Security Requirements and Guidelines for Application Vendors and Application Service Providers

07/2015

Table of Contents

1 Overview

Security Requirements and Guidelines for Application Vendors and Application Service Providers

This document provides a high-level overview of application security related guidelines and requirements set forth by the Orange County Health Care Agency (OCHCA), and applies to both software vendors for County-implemented applications and application service providers who provide hosted services.

These requirements and guidelines are consistent with regulatory privacy and security requirements and guidelines as well as supportive of OCHCA's position and practices on risk management in terms of appropriately safeguarding OCHCA's information assets.

The sections below are comprehensive and may apply in whole or in part based on specific implementation and scope of work. The expectation is that vendors will comply with relevant sections, as necessary. This information will be reviewed, validated and documented by OCHCA Security prior to any contract being finalized.

Vendors are required to comply with all existing legal and regulatory requirements as they relate to OCHCA's systems and data. Example of regulations, rules and laws include, but are not limited to, the Health Insurance Portability and Accountability Act (HIPAA), Senate Bill 1386, Payment Card Industry (PCI) Data Security Standards, and SarbanesOxley (SOX). Vendors must also commit to ensuring compliance with all future local, state and federal laws and regulations related to privacy and security as they pertain to the application or service.

2 General Security Requirements

- The application/system must meet the general security standards based upon ISO 17799 – Code of Practice for Information Security and ISO 27799 – Security Management in Health Using ISO 17799.
- The application must run on an operating system that is consistently and currently supported by the operating systems vendor. Applications under maintenance are expected to always be current in regards to the current version of the relevant operating system.
- For applications hosted by OCHCA, OCHCA will routinely apply patches to both the operating system and subsystems as updated releases are available from the operating system vendor and or any third party vendors. The vendors must keep their software current and compatible with such updated releases in order for the application to operate in this environment.
- Vendors must provide timely updates to address any applicable security vulnerabilities found in the application.
- OCHCA utilizes a variety of proactive, generally available, monitoring tools to assess and manage the health and performance of the application server, network connectivity, power etc. The application must function appropriately while the monitoring tools are actively running.
- All application services must run as a true service and not require a user to be logged into the application for these services to continue to be active. OCHCA will provide an account with the appropriate security level to logon as a service, and an account with the appropriate administrative rights to administer the application. The account password must periodically expire, as per OCHCA policies and procedures.

- In order for the application to run on OCHCA server and network resources, the application must not require the end users to have administrative rights on the server or subsystems.

3 Encryption

- Application/system must use encryption to protect sensitive data at rest wherever technically possible (e.g. SQL TDE Encryption).
- All data transmissions must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end to end at the network level. This requirement pertains to any regulated data in motion such as website access and file transfers.
- All electronic files, where applicable, that contain OCHCA data must be encrypted when stored on any removable media or portable device (USB drives, CD/DVD, mobile phones, backup tapes). The encryption must be a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher.
- All encryption methods used for data storage and transmission must be disclosed by the vendors.

4 Network Application Documentation

- Vendors must provide documentation related to the configuration of the application including methods of secure implementation and port requirements.

5 Access Management

- Application/system must control access to and within the system at multiple levels (e.g. per user, per user role, per area, per section of the chart) through a consistent mechanism of identification and authentication of all users in accordance with the 'Role Based Access Control' (RBAC) standard.
- Application/system must support measures to define, attach, modify and remove access rights for all classes of users.
- Application/system must support measures to enable and restrict access to the whole and/or sections of the technology solution in accordance with prevailing consent and access rules.
- Application must have the ability to create unique user accounts.
- Application must support session timeouts or automatic logoff after 20 minutes of inactivity.
- The application must provide functionality to automatically disable or lock accounts after 60 days of inactivity.

6 Password Management

- Application must support password management measures including but not limited to password expiration, account lockout and complex passwords.
- Passwords expiration must be set to 90 days and the system must prevent the use of the previous 4 passwords.

- Accounts must be locked after five unsuccessful login attempts.
- The password must be at least 8 characters in length and a combination of letters, numbers, and special characters with at least 3 of the four following categories.
    - Uppercase letters (A through Z)
    - Lowercase letters (a through z)
    - Numeric digits (0 through 9)
    - Special Characters (! @ # $ % ^ & etc.)

7 Audit Capabilities

Auditing and logging capabilities will permit HCA to identify, and possibly reverse, unauthorized or unintended changes to application.

- Application must support the identification of the nature of each access and/or modification through the use of logging.
- Application must employ audit capabilities to sufficiently track details that can establish accountability for each step or task taken in a clinical or operational process.
- All audit logs must be protected from human alteration.
- Access to logs must be limited to authorized users.
- The application must employ basic query tools and reports to easily search logs.
- OCHCA record retention policies must be followed. Currently OCHCA requires that this period be at least six years from the time the record was initiated.
- Logging and auditing functionality must include the following:
    - Record of who did what to which object, when and on which system.
    - Successful/unsuccessful log-in and log-out of users.
    - Add, modify and delete actions on data/files/objects.
    - Read/view actions on data classified as restricted/confidential.
    - Changes to user accounts or privileges (creation, modification, deletion).
    - Switching to another users access or privileges after logging in (if applicable).

8 Protection from Malicious Code

- For cloud hosted solutions, vendors must utilize antivirus/antispyware software on servers and monitor to prevent malicious code which may lead to a compromise of OCHCA's data.
- For local hosted solutions, vendors must ensure that the application appropriately supports the use of antivirus/antispyware software.

9 Remote Support Functionality

- Provider must conform to OCHCA Vendor Remote Access Policy.

10 HCA Data Usage

- During the course of any implementation and subsequent support and life cycle management, any OCHCA data that the vendors have access to in any manner shall be considered confidential unless otherwise designated in writing.
- Vendors must not use or disclose OCHCA's data other than as permitted or as required by contract or law.
- The vendors must agree to use appropriate safeguards to prevent the unauthorized use or disclosure of OCHCA's data during any time that the data is stored or transported in any manner by vendors.
- After the end of any appropriate use of OCHCA's data within the vendors' possession, such data must be returned to OCHCA or securely destroyed unless otherwise permitted by contract or law.

11 Cloud Solutions

Application Service Providers hosting OCHCA data must meet the following additional requirements and are required to comply with and provide deliverables noted below:

- Network Intrusion Detection and Prevention. All systems that are accessible via the internet must actively use a network based intrusion detection and prevention solution.
- Workstation/Laptop Encryption. All workstations, laptops and mobile devices that process and/or store OCHCA data must be encrypted using full disk encryption that uses a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher.
- Patch Management. All workstations, laptops, and other systems that access, process and/or store OCHCA data must have appropriate security patches installed. Application Service Providers must utilize a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a minimum, all applicable patches must be installed within 30 days of vendor release.
- Application Access. All systems accessible via the internet must employ security controls to prevent access to the application via an asset not approved or owned by the county.
- Risk Assessment. Application Service Providers hosting data for HIPAA covered services must conduct an accurate and thorough Risk Assessment as required by HIPAA Security Rule, Security Management (§ 164.308(a)(1)). Further, they must follow the risk assessment methodology, based on the latest version of NIST SP 800-30 (http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf). Upon request, the Risk Assessment findings and remediation strategy must be shared with OCHCA.
- NIST. To ensure compliance with HIPAA, Application Service Providers shall implement appropriate security safeguards by following National Institute of Standards and Technology (NIST) guidelines.

12 Policies

Vendors must have formal, published IT security policies that address how they manage and maintain the internal security posture of their own or sub-contracted infrastructure. The vendor shall also clearly demonstrate that additional security features are in place to protect systems and data in the unique environment of the service provider model: namely, security issues associated with storing County-owned data on a remote server that is not under direct County control and the necessity of transferring this data over an untrusted network.

Vendors must provide, to the extent permissible, all relevant security policies and procedures to the County for review and validation. All documentation must be provided in electronic format for the County's review.

These policies must include, but not be limited to, the following:

- IT Staff Usage Agreement. All vendor employees performing services for the County must sign and agree to an IT usage agreement within their own organization as part of an overall security training and awareness program. At a minimum, vendor employees must sign a statement of understanding within their own organization regarding Internet dangers, IT security, and IT ethics and best practices,

- IT Security Policies and Procedures.

- IT Operations Security Policy. Written standards for operational security for any facilities where the County data, staff or systems shall exist. These documents must include, but not be limited to, physical security, network security, logical security, systems/platform security, wireless access, remote access, and data protections.

- Data Management Security Policy. Policy for the safeguarding and management of all data provided by the County or accessed by vendor as part of implementation and ongoing maintenance. This policy must, at a minimum, include check-in, check-out, copy control, audit logs and separation of duties.

- Security Incident Notification and Management Process. A detailed document that outlines the contact names and order and escalation of events that will occur in the case of a security breach concerning the County staff, data, or systems. This document must be updated immediately upon any change. The vendor shall be held liable to the time-tables and protections outlined in the document.

In addition to developing, maintaining, and enforcing the above named policies, the vendor must:

- Bear the cost of compliance for any required changes to security infrastructure, policies and procedures to comply with existing regulations, unless such change is unique to the County.
- Comply with reasonable requests by the County for audits of security measures, including those related to identification and password administration.

- Comply with reasonable requests by the County for onsite physical inspections of the location from which the vendor provides services.
- Provide the County with any annual audit summaries and certifications, including but not limited to HIPAA, ISO or SOX audits, as applicable.
- Designate a single point of contact to facilitate all IT security activities related to services provided to the County, with the allowance of appropriate backups. Such contact(s) must be available on a 7/24/365 basis.

13 Business Continuity / Disaster Recovery Plans

Application Service Providers must have a viable risk management strategy that is formally documented in a Business Continuity Plan (BCP) and/or a Disaster Recovery Plan (DRP). This BCP/DRP plan(s) must identify recovery strategies within the application service areas, outline specific recovery methods and goals, and provide the mutually agreed upon recovery time and point objectives.

14 Backup and Restore

The vendor must provide their routine Backup and Restore policy and procedure which includes their backup data security strategy. These procedures shall allow for protection of encryption keys (if applicable) as well as a document media destruction strategy including media management tasks (i.e., offsite vaulting and librarian duties).

15 Staff Verification

For any employee a vendor contemplates using to provide services for the County, the vendor shall use its standard employment criteria as used for similar services provided to other customers in evaluating the suitability of that employee for such roles.

At a minimum, subject to the requirements of applicable law, such criteria must include the information as outlined below for each employee:

- Relevant Skills, Licenses, Certifications, Registrations. Each service employee must possess the educational background, work experience, skills, applicable professional licenses, and related professional certifications commensurate with their position. The County may, at any time and at its sole discretion, request that the vendor demonstrate compliance with this requirement as applicable to the nature of the services to be offered by the vendor's employee. The County may, at its sole discretion, also request the vendor's certification that the vendor employee has undergone a chemical/drug screening, with negative results, prior to granting access to the County facilities.

- Background Checks. In accordance with applicable law, the vendor must, at the County's request, obtain as a condition of employment, a background investigation on any vendor employee selected to work for the County. The security and background investigation shall include criminal record checks, including records of any conviction in the U.S. or other relevant jurisdiction where the employee resides. Costs for background investigations must be borne by the vendor.

At a minimum, subject to the requirements of applicable law, the vendor must:

1. Ensure that all vendor service employees performing applicable services or supporting the vendor's duties and obligations under a County agreement: (i) have not been convicted of any crime involving violence, fraud, theft, dishonesty or breach of trust under any laws; and (ii) have not been on any list published and maintained by the Government of the United States of America of persons or entities with whom any United States person or entity is prohibited from conducting business.

2. Follow such verification procedures as may be reasonably specified by the County from time to time. If either the vendor or the County becomes aware that any vendor employee has been convicted of a crime involving violence, fraud, theft, dishonesty or breach of trust, or has been included on any such list of persons or entities convicted of such crimes, then the vendor shall promptly remove the employee from providing services to the County and prohibit that employee from entering any facilities at which services are provided.

3. Annually certify to the County that, to the best of its knowledge, none of the service employees have been convicted of any felony involving fraud, theft, dishonesty or a breach of trust under any laws.

16 IT Physical Security and Access Control

The vendor must establish processes and procedures for physical access to and control of their own facilities that are, at a minimum, consistent with relevant industry-specific best practices.

Vendor employees are expected to:

- Comply with facility access procedures, using procedures such as sign-in/sign-out requirements and use of assigned ID badges.
- Scan ID badges, where applicable, at any secure door and/or entrance and exit gates, including any door or gate that may already be open.
- Refrain from using recordable media in conjunction with County-owned equipment.
- Comply with check-in/check-out requirements for materials and/or equipment.
- Adhere to the facility's established emergency, safety and evacuation procedures.
- Report any unsafe conditions to the facility's safety representative.
- Report any access violations or security threats to the facility's local security administrator.

17 IT Security Compliance and Training

The vendor must ensure that all vendor employees comply with security policies and procedures and take all reasonable measures to reduce the opportunity for unauthorized access, transmission, modification or misuse of the County's data by vendor employees.

The vendor must ensure that all vendor employees are trained on security measures and practices. The vendor will be responsible for any costs related to such training.

At a minimum, the vendor is expected to:

- Ensure that a formal disciplinary process is defined and followed for vendor employees who violate established security policies and procedures.
- Proactively manage and administer access rights to any equipment, software and systems used to provide services to the County.
- Define, maintain and monitor access controls, ranging from physical access to logical security access, including a monthly review of vendor employees' access to systems used to provide services to the County.

The vendor shall monitor facilities, systems and equipment to protect against unauthorized access.

At a minimum, the vendor is expected to:

- Monitor access to systems; investigate apparent security violations; and notify the County of suspected violations, including routine reporting on hacking attempts, penetrations and responses.
- Maintain data access control and auditing software and provide adequate logging, monitoring, and investigation of unusual or suspicious activity.
- Initiate immediate corrective actions to minimize and prevent the reoccurrence of attempted or actual security violations.
- Document details related to attempted or actual security violations and provide documentation to the County.
- Provide necessary documentation and evidence to the County in connection with any legal action or investigation.

18 Security Testing Recommendations

The vendor should perform a series of steps to verify the security of applications, some of which are noted below. This section will not be validated by the County, but reflects best practices that the vendor should consider and follow.

1. Look for vulnerabilities at various layers of the target environment. In the lowest layer, the vendor's testing team should look for flaws in the target network environment, including any routers and firewalls designed to control access to the web server and related target components. The team should attempt to determine whether such filters provide adequate protection at the network layer of the target hosts that the team can reach across the Internet.
2. Look for flaws in the Internet-accessible hosts associated with the target infrastructure, including the web server. This host-based component of the test will analyze which network-accessible services are available on the target hosts across the Internet, including the web

server process. The testing team should look for incorrect configuration, unpatched or enabled services, and other related problems on the target hosts.

This review performed by the vendor should include but not be limited to:

- The web application (i.e., the software that interacts with users at their web browsers; typically customcrafted code created by the web development team)
- The web server application (the underlying software that sends and receives information via HTTP and HTTPS, typically off-the-shelf software such as Microsoft's IIS or the open-source Apache software)
- Any separate backend application servers that process information from the web application
- The backend database systems that house information associated with the web application.
- Infrastructure diagrams.
- Configuration host review of settings and patch versions, etc.
- Full code review.
- Identification and remediation of well-known web server, code engine, and database vulnerabilities.
- Identification and remediation of any server and application administration flaws and an exploitation attempt of same.
- Analysis of user interface, normal application behavior, and overall application architecture for potential security vulnerabilities.
- Analysis of data communications between the application and databases or other backend systems.
- Manual analyses of all input facilities for unexpected behavior such as SQL injection, arbitrary command execution, and unauthorized data access.
- Analyses of user and group account authentication and authorization controls to determine if they can be bypassed.
- Identification of information leakage across application boundaries, including the capability to enumerate other users' data and "show code" weaknesses that reveal internal application logic.
- Identification of areas where error handling is insufficient or reveals too much sensitive information.
- Identification of opportunities to write to the host file system or execute uploaded files.
- Identification of product sample files, application debugging information, developer accounts or other legacy functionality that allows inappropriate access.
- Determination as to whether or not fraudulent transactions or access can be performed.
- Attempts to view unauthorized data, especially data that should be confidential.
- Examination of client-side cached files, temporary files, and other information that can yield sensitive information or be altered and re-submitted.
- Analysis of encoded and encrypted tokens, such as cookies, for weakness or the ability to be reverse engineered.

19 Vendor Deliverables

The following items are to be provided by the vendor prior to the contract finalization:

- OCHCA Security Requirements and Guidelines for Application Vendors and Application Service Providers – Questionnaire
- Vendor risk acceptance / compliance statement
- Business Continuity Plan Summary (as related to service provided)
- ISO SOX compliance certificate (if applicable)
- Security Waiver form (if applicable)
- IT Security Staff Usage Policy
- IT Security Policies and Procedures
- IT Operations Security Policy
- Data Management Security Policy
- Security Incident Notification and Management Process
- Security Contact Identification (24x7x365)
- Staff Related Items
    - Pre-Employment Screening Policy/Procedure
    - Background Checking Procedure
    - Ongoing Employment Status Validation Process
    - Staff Roster and Duties