CONTRACT NO. MA-042-21010462

FOR

NURSE CASE MANAGEMENT SYSTEM
BETWEEN

THE COUNTY OF ORANGE
HEALTH CARE AGENCY

AND

NETCHEMISTRY, INC.

CONTRACT NO. MA-042-21010462
FOR
NURSE CASE MANAGEMENT SYSTEM
WITH
NETCHEMISTRY, INC.

This Contract Number MA-042-21010462 ("Contract"), is made and entered into this _________ day of _______, 2020 ("Effective Date") between **NetChemistry, Inc.** ("Contractor"), with a place of business at 4600 Campus Drive, Suite 101, Newport Beach, CA 92660 and County of Orange, a political subdivision of the State of California ("County"), through its Health Care Agency with a place of business at 200 Santa Ana Blvd., Suite 650, Santa Ana, CA 92701-7506. Contractor and County may sometimes be referred to hereinafter individually as "Party" or collectively as "Parties.

ATTACHMENTS

This Contract is comprised of this document and the following Attachments, which are attached hereto and incorporated by reference into this Contract:

Attachment A – Scope of Work
Attachment B – Contractor's Scope of Work
Attachment C – Compensation & Invoicing
Attachment D – Cost Summary/Pricing
Attachment E – Business Associate Contract
Attachment E1- Personal Information Privacy and Security Contract
Attachment F – OCHCA Security Requirements and Guidelines for Contractors and Application Service Providers

RECITALS

WHEREAS, County issued a Request for Proposals (RFP) for an Nurse Case Management System; and

WHEREAS, Contractor responded and represented that its proposed services shall meet or exceed the requirements and specifications of the RFP; and

WHEREAS, Contractor agrees to provide services to the County as further set forth in the Scope of Work, attached hereto as Attachment A; and

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

WHEREAS, County of Orange Board of Supervisors has authorized the County Procurement Officer or designee to enter into a Contract for Nurse Case Management System with the Contractor;

NOW, THEREFORE, the Parties mutually agree as follows:

DEFINITIONS

DPA shall mean the Deputy Purchasing Agent assigned to this Contract.

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 adjudication to another county.

B. **Entire Contract:** This Contract 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 DPA designee.

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's Purchasing Agent or DPA designee in writing.

D. **Taxes:** Unless otherwise provided herein or by law, price quoted does not include California state sales or use tax. Out-of-state Contractors shall indicate California Board of Equalization permit number and sales permit number on invoices, if California sales tax is added and collectable. If no permit numbers are shown, sales tax will be deducted from payment. The Auditor-Controller will then pay use tax directly to the State of California in lieu of payment of sales tax to the Contractor.

E. **Delivery:** Time of delivery of goods or services is of the essence in this Contract. County reserves the right to refuse any goods or services and to cancel all or any part of the goods not conforming to applicable specifications, drawings, samples or descriptions or services that do not conform to the prescribed statement of work. Acceptance of any part of the order for goods shall not bind County to accept future shipments nor deprive it of the right to return goods already accepted at Contractor's expense. Over shipments and under shipments of goods shall be only as agreed to in writing by County. Delivery shall not be deemed to be complete until all goods or services have actually been received and accepted in writing by County.

F. **Acceptance/Payment:** Unless otherwise agreed to in writing by County, 1) acceptance shall not be deemed complete unless in writing and until all the goods/services have actually been received, inspected, and tested to the satisfaction of County, and 2) payment shall be made in arrears after satisfactory acceptance.

G. **Warranty**: Contractor expressly warrants that the goods covered by this Contract are 1) free of liens or encumbrances, 2) merchantable and good for the ordinary purposes for which they are used, and 3) fit for the particular purpose for which they are intended. Acceptance of this order shall constitute an agreement upon Contractor's part to indemnify, defend and hold County and its indemnities as identified in paragraph "Z" below, and as more fully described in paragraph "Z," harmless from liability, loss, damage and expense, including reasonable counsel fees, incurred or sustained by County by reason of the failure of the goods/services to conform to such warranties, faulty work performance, negligent or unlawful acts, and non-compliance with any applicable state or federal codes, ordinances, orders, or statutes, including the Occupational Safety and Health Act (OSHA) and the California Industrial Safety Act. Such remedies shall be in addition to any other remedies provided by law.

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, proprietary right, or trade secret right of any third party. Contractor agrees that, in accordance with the more specific requirement contained in paragraph "Z" below, it shall indemnify, defend and hold County and County Indemnitees harmless from any and all such claims and be responsible for payment of all costs, damages, penalties and expenses related to or arising from such claim(s), including, costs and expenses but not including attorney's fees.

I. **Assignment:** 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 by Contractor without the express written consent of County. Any attempt by Contractor to assign 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.

J. **Non-Discrimination:** In the performance of this Contract, Contractor agrees that it will 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, marital status, or sex of such persons. Contractor acknowledges that a violation of this provision shall subject Contractor to penalties pursuant to Section 1741 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 immediately terminate this Contract without penalty for cause or after 30 days' written notice without cause, unless otherwise specified. Cause shall be defined as any material breach of contract, any misrepresentation or fraud on the part of the Contractor. Exercise by County of its right to terminate the Contract shall relieve County of all further obligation.

Upon notification of contract termination, the Contractor will make available, via secure FTP (SFTP), an unencrypted full Production backup in MS SQL file format or XML (SQL preferred), of all county data, related metadata and associated database schema within 45 days.

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. **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.

N. **Performance Warranty:** Contractor shall warrant 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 goods/services furnished by the Contractor under this Contract. Contractor shall perform all work diligently, carefully, and in a good and workmanlike manner; shall furnish all necessary labor, supervision, machinery, equipment, materials, and supplies, 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. If permitted to subcontract, Contractor shall be fully responsible for all work performed by subcontractors.

O. **Insurance Provisions:** Prior to the provision of services under this Contract, the Contractor agrees to purchase all required insurance at Contractor's expense, including all endorsements required herein, necessary to satisfy the County that the insurance provisions of this Contract have been complied with. Contractor agrees to keep such insurance coverage, Certificates of Insurance, and endorsements on deposit with the 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.

Contractor shall ensure that all subcontractors performing work on behalf of Contractor pursuant to this Contract shall be covered under Contractor's insurance as an additional insured or maintain insurance subject to the same terms and conditions as set forth herein for Contractor. Contractor shall not allow subcontractors to work if subcontractors have less than the level of coverage required by County from Contractor under this Contract. It is the obligation of Contractor to provide notice of the insurance requirements to every subcontractor and to receive proof of insurance prior to allowing any subcontractor to begin work. Such proof of insurance must be maintained by Contractor through the entirety of this Contract for inspection by County representative(s) at any reasonable time.

All self-insured retentions (SIRs) shall be clearly stated on the Certificate of Insurance. Any self-insured retention (SIR) in an amount in excess of Fifty Thousand Dollars ($50,000) shall specifically be approved by the County's Risk Manager, or designee, upon review of Contractor's current audited financial report. If Contractor's SIR is approved, Contractor, in addition to, and without limitation of, any other indemnity provision(s) in this Contract, agrees to all of the following:

1) In addition to the duty to indemnify and hold the County harmless against any and all liability, claim, demand or suit resulting from Contractor's, its agent's, employee's or subcontractor's performance of this Contract, Contractor shall defend the County at its sole cost and expense with counsel approved by Board of Supervisors against same; and
2) Contractor's duty to defend, as stated above, shall be absolute and irrespective of any duty to indemnify or hold harmless; and
3) The provisions of California Civil Code Section 2860 shall apply to any and all actions to which the duty to defend stated above applies, and the Contractor's SIR provision shall be interpreted as though the Contractor was an insurer and the County was the insured.

If the Contractor fails to maintain insurance acceptable to the County for the full term of this Contract, the County may terminate this Contract.

Qualified Insurer

The policy or policies of insurance must be issued by an insurer with a minimum rating of 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).** It is preferred, but not mandatory, that the insurer be licensed to do business in the state of California (California Admitted Carrier).

If the insurance carrier does not have an A.M. Best Rating of A-/VIII, the 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 the 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 for owned, non-owned and hired vehicles	$1,000,000 per occurrence
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:

1) An Additional Insured endorsement using ISO form CG 20 26 04 13 or a form at least as broad naming the ***County of Orange its elected and appointed officials, officers, agents and employees*** as Additional Insureds, or provide blanket coverage, which will state ***AS REQUIRED BY WRITTEN CONTRACT***.

2) A primary non-contributing endorsement using ISO form CG 20 01 04 13, or a form at least as broad evidencing that the Contractor's insurance is primary and any insurance or self-insurance maintained by the 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 the Contractor's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

The Workers' Compensation policy shall contain a waiver of subrogation endorsement waiving all rights of subrogation against the ***County of Orange, its elected and appointed officials, officers, agents and employees*** or provide blanket coverage, which will state **AS REQUIRED BY WRITTEN CONTRACT.**

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

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 the 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 interest’s 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 the Contractor fails to provide the insurance certificates and endorsements within seven (7) days of notification by CEO/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 will 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.

P. **Changes:** Contractor shall make no changes in the work or perform any additional work without the Deputy Purchasing Agent’s specific written approval.

Q. **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.

R. **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 36 hours of the start of the delay and Contractor avails himself of any available remedies.

S. **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.

T. **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. Contractor acknowledges that County is relying on Contractor to ensure such compliance, and pursuant to the requirements of paragraph "Z" below, Contractor agrees that it shall defend, indemnify and hold County and County Indemnitees harmless from all liability, damages, costs and expenses arising from or related to a violation of such laws.

U. **Freight:** Prior to the County's express acceptance of delivery of products. 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.

V. **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.

W. **Attorney Fees:** In any action or proceeding to enforce or interpret any provision of this Contract, each Party shall bear their own attorney's fees, costs and expenses.

X. **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 had been represented by experienced and knowledgeable independent legal counsel of their 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 they have not been influenced to any extent whatsoever in executing this Contract by any other Party hereto or by any person representing them, or both. Accordingly, any rule or 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.

Y. **Employee Eligibility Verification:** The 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. The 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. The Contractor shall retain all such documentation for all covered employees for the period prescribed by the law. The Contractor shall indemnify, defend with counsel approved in writing by County, and hold harmless, the County, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against the Contractor or the County or both in connection with any alleged violation of any Federal or State statutes or regulations pertaining to the eligibility for employment of any persons performing work under this Contract.

Z. **Indemnification:** Contractor agrees to indemnify, defend with counsel approved in writing by County, and hold County, its elected and appointed officials, officers, employees, agents and those special districts and agencies 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 or property damage, arising from or related to 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 will be apportioned as determined by the court. Neither Party shall request a jury apportionment.

AA. **Audits/Inspections:** Contractor agrees to permit the County's Auditor-Controller or the Auditor-Controller's authorized representative (including auditors from a private auditing firm hired by the 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 will be confined to those matters connected with the performance of the Contract including, but not limited to, the costs of administering the Contract. The County will provide reasonable notice of such an audit or inspection.

The County reserves the right to audit and verify the Contractor's records before final payment is made.

Contractor agrees to maintain such records for possible audit for a minimum of three 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 or others who might reasonably have information related to such records. Further, Contractor agrees to include a similar right to the County to audit records and interview staff of any subcontractor related to performance of this Contract.

Should the Contractor cease to exist as a legal entity, the Contractor's records pertaining to this agreement shall be forwarded to the County's project manager.

BB. **Contingency of Funds:** Contractor acknowledges that funding or portions of funding for this Contract may be contingent upon state budget approval; receipt of funds from, and/or obligation of funds by, the State of California to County; and inclusion of sufficient funding for the services hereunder in the budget approved by County's Board of Supervisors for each fiscal year covered by this Contract. If such approval, funding or appropriations are not forthcoming, or are otherwise limited, County may immediately terminate or modify this Contract without penalty.

CC. **Expenditure Limit:** The Contractor shall notify the County of Orange assigned Deputy Purchasing Agent in writing when the expenditures against the Contract reach 75 percent of the dollar limit on the Contract. The County shall not be responsible for any expenditure overruns and will not pay for work exceeding the dollar limit on the Contract unless a change order to cover those costs has been issued.

Additional Terms and Conditions

1. **Scope of Contract**: This Contract specifies the contractual terms and conditions by which the County shall procure nurse case management system from Contractor as further detailed in the Scope of Work, identified and incorporated herein by this reference as "Attachment A".

2. **Term of Contract:** This Contract shall commence on **December 16, 2020** through and including **December 15, 2025**, non-renewable. The 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.

3. **Breach of Contract:** The failure of the 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 the County may, and in addition to any other remedies available at law, in equity, or otherwise specified in this Contract:

   a) Terminate the Contract immediately, pursuant to Section K herein;

   b) Afford the 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;

   c) Discontinue payment to the Contactor for and during the period in which the Contractor is in breach; and

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

4. **Civil Rights:** Contractor attests that services provided shall be in accordance with the provisions of Title VI and Title VII of the Civil Rights Act of 1964, as amended, Section 504 of the Rehabilitation Act of 1973, as amended; the Age Discrimination Act of 1975 as amended; Title II of the Americans with Disabilities Act of 1990, and other applicable State and federal laws and regulations prohibiting discrimination on the basis of race, color, national origin, ethnic group identification, age, religion, marital status, sex or disability.

5. **Conflict of Interest – Contractor's Personnel**: The Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of the County. This obligation shall apply to the Contractor; the Contractor's employees, agents, and subcontractors associated with accomplishing work and services hereunder. The Contractor's efforts shall include, but not be limited to establishing precautions to prevent 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 from acting in the best interests of the County.

6. **Conflict of Interest – County Personnel:** The County of Orange Board of Supervisors policy prohibits its employees from engaging in activities involving a conflict of interest. The Contractor shall not, during the period of this Contract, employ any County employee for any purpose.

7. **Contractor's Project Manager and Key Personnel:** Contractor shall appoint a Project Manager to direct the Contractor's efforts in fulfilling Contractor's obligations under this Contract. This Project Manager shall be subject to approval by the County and shall not be changed without the written consent of the County's Project Manager, which consent shall not be unreasonably withheld.

   The Contractor's Project Manager shall be assigned to this project for the duration of the Contract and shall diligently pursue all work and services to meet the project time lines. The County's Project Manager shall have the right to require the removal and replacement of the Contractor's Project Manager from providing services to the County under this Contract. The County's Project manager shall notify the Contractor in writing of such action. The Contractor shall accomplish the removal within five (5) business days after written notice by the County's Project Manager. The County's Project Manager shall review and approve the appointment of the replacement for the Contractor's Project Manager. The County is not required to provide any additional information, reason or rationale in the event it The County is not required to provide any additional information, reason or rationale in the event it requires the removal of Contractor's Project Manager from providing further services under the Contract.

8. **Contractor's Records:** The Contractor shall keep true and accurate accounts, records, books and data which shall correctly reflect the business transacted by the 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 the County. Storage of records in another county will require written approval from the County of Orange assigned Deputy Purchasing Agent.

9. **Conditions Affecting Work:** The Contractor shall be responsible for taking all steps reasonably necessary to ascertain the nature and location of the work to be performed under this Contract and to know the general conditions which can affect the work or the cost thereof. Any failure by the Contractor to do so will not relieve Contractor from responsibility for successfully performing the work without additional cost to the County. The County assumes no responsibility for any understanding or representations concerning the nature, location(s) or general conditions made by any of its officers or agents prior to the execution of this Contract, unless such understanding or representations by the County are expressly stated in the Contract.

10. **Cooperative Contract:** The provisions and pricing of this Contract will be extended to other California local or state governmental entities. Governmental entities wishing to use this Contract will be responsible for issuing their own purchase documents/price agreements, providing for their own acceptance, and making any subsequent payments. Contractor shall be required to include in any Contract entered into with another agency or entity that is entered into as an extension of this Contract a Contract clause that will hold harmless the County of Orange from all claims, demands, actions or causes of actions of every kind resulting directly or indirectly, arising out of, or in any way connected with the use of this contract. Failure to do so will be considered a material breach of this Contract and grounds for immediate Contract termination. The cooperative entities are responsible for obtaining all certificates of insurance and bonds required. The Contractor is responsible for providing each cooperative entity a copy of the Contract upon request by the cooperative entity. The County of Orange makes no guarantee of usage by other users of this Contract.
The Contractor shall be required to maintain a list of the cooperative entities using this Contract. The list shall report dollar volumes spent annually and shall be provided on an annual basis to the County, at the County's request.

11. **Data – Title To:** All materials, documents, data or information obtained from the County data files or any County medium furnished to the Contractor in the performance of this Contract will at all times remain the property of the County. Such data or information may not be used or copied for direct or indirect use by the Contractor after completion or termination of this Contract without the express written consent of the County. All materials, documents, data or information, including copies, must be returned to the County at the end of this Contract.

12. **Default – Reprocurement Costs:** In case of Contract breach by Contractor, resulting in termination by the County, the County may procure the goods and/or services from other sources. If the cost for those goods and/or services is higher than under the terms of the existing Contract, Contractor will be responsible for paying the County the difference between the Contract cost and the price paid, and the County may deduct this cost from any unpaid balance due the Contractor. The price paid by the County shall be the prevailing market price at the time such purchase is made. This is in addition to any other remedies available under this Contract and under law.

13. **Disputes – Contract:**

A. 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 the Contractor's Project Manager and the County's Project Manager, such matter shall be brought to the attention of the County Deputy Purchasing Agent by way of the following process:

1. The Contractor shall submit to the agency/department assigned Deputy Purchasing Agent 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 the County, on its own initiative, has already rendered such a final decision.

2. The Contractor's written demand shall be fully supported by factual information, and, if such demand involves a cost adjustment to the Contract, the 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 the Contractor believes the County is liable.

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

Any final decision of the County shall be expressly identified as such, shall be in writing, and shall be signed by the County Deputy Purchasing Agent or his designee. If the County fails to render a decision within 90 days after receipt of the Contractor's demand, it shall be deemed a final decision adverse to the Contractor's contentions. Nothing in this section shall be construed as affecting the County's right to terminate the Contract for cause or termination for convenience as stated in section K herein.

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

1. 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)(1).

2. Establish a drug-free awareness program as required by Government Code Section 8355(a)(2) to inform employees about all of the following:
   a. The dangers of drug abuse in the workplace;

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

   c. Any available counseling, rehabilitation and employee assistance programs; and

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

3. Provide as required by Government Code Section 8355(a)(3) that every employee who works under this Contract:

   a. Will receive a copy of the company's drug-free policy statement; and

b. Will 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 the Contractor may be ineligible for award of any future County contracts if the County determines that any of the following has occurred:

1. The Contractor has made false certification, or

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

15. **EDD Independent Contractor Reporting Requirements:** Effective January 1, 2001, the County of Orange is required to file in accordance with subdivision (a) of Section 6041A of the Internal Revenue Code for services received from a "service provider" to whom the County pays $600 or more or with whom the 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 Contractors. 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 http://www.edd.ca.gov/Employer_Services.htm

16. **Emergency/Declared Disaster Requirements:** In the event of an emergency or if Orange County is declared a disaster area by the County, state or federal government, this Contract may be subjected to unusual usage. The Contractor shall service the County during such an emergency or declared disaster under the same terms and conditions that apply during non-emergency/disaster conditions. The pricing quoted by the Contractor shall apply to serving the County's needs regardless of the circumstances. If the Contractor is unable to supply the goods/services under the terms of the Contract, then the Contractor shall provide proof of such disruption and a copy of the invoice for the goods/services from the Contractor's supplier(s). Additional profit margin as a result of supplying goods/services during an emergency or a declared disaster shall not be permitted. In the event of an emergency or declared disaster, emergency purchase order numbers will be assigned. All applicable invoices from the Contractor shall show both the emergency purchase order number and the Contract number.

17. **Errors and Omissions:** All reports, files and other documents prepared and submitted by Contractor shall be complete and shall be carefully checked by the professional(s) identified by Contractor as project manager and key personnel attached hereto, prior to submission to the County. Contractor agrees that County review is discretionary and Contractor shall not assume that the County will discover errors and/or omissions. If the County discovers any errors or omissions prior to approving Contractor's reports, files and other written documents, the reports, files or documents will be returned to Contractor for correction. Should the County or others discover errors or omissions in the reports, files or other written documents submitted by the Contractor after County approval thereof, County approval of Contractor's reports, files or documents shall not be used as a defense by Contractor in any action between the County and Contractor, and the reports, files or documents will be returned to Contractor for correction.

18. **Equal Employment Opportunity:** The Contractor shall comply with U.S. Executive Order 11246 entitled, "Equal Employment Opportunity" as amended by Executive Order 11375 and as supplemented in Department of Labor regulations (41 CFR, Part 60) and applicable State of California regulations as may now exist or be amended in the future. The Contractor shall not discriminate against any employee or applicant for employment on the basis of race, color, national origin, ancestry, religion, sex, marital status, political affiliation or physical or mental condition.

    Regarding handicapped persons, the Contractor will not discriminate against any employee or applicant for employment because of physical or mental handicap in regard to any position for which the employee or applicant for employment is qualified. The Contractor agrees to provide equal opportunity to handicapped persons in employment or in advancement in employment or otherwise treat qualified handicapped individuals without discrimination based upon their physical or mental handicaps in all employment practices such as the following: employment, upgrading, promotions, transfers, recruitments, advertising, layoffs, terminations, rate of pay or other forms of compensation, and selection for training, including apprenticeship. The Contractor agrees to comply with the provisions of Sections 503 and 504 of the Rehabilitation Act of 1973, as amended, pertaining to prohibition of discrimination against qualified handicapped persons in all programs and/or activities as detailed in regulations signed by the Secretary of the Department of Health and Human Services effective June 3, 1977, and found in the Federal Register, Volume 42, No. 68 dated May 4, 1977, as may now exist or be amended in the future.

    Regarding Americans with disabilities, Contractor agrees to comply with applicable provisions of Title 1 of the Americans with Disabilities Act enacted in 1990 as may now exist or be amended in the future.

19. **News/Information Release:** The Contractor agrees that it will not issue any news releases 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 of said news releases from the County through the County's Project Manager.

20. **Notices:** Any and all notices, requests demands and other communications contemplated, called for, permitted, or required to be given hereunder shall be in writing with a copy provided to the assigned Deputy Purchasing Agent (DPA), except through the course of the parties' project managers' routine exchange of information and cooperation

during the terms of the work and services. Any written communications shall be deemed to have been duly given upon actual in-person delivery, if delivery is by direct hand, or upon delivery on the actual day of receipt or no greater than four (4) calendar days after being mailed by US certified or registered mail, return receipt requested, postage prepaid, whichever occurs first. The date of mailing shall count as the first day. All communications shall be addressed to the appropriate Party at the address stated herein or such other address as the parties hereto may designate by written notice from time to time in the manner aforesaid.

For Contractor: Name: NetChemistry, Inc.
Attention: Chris Cruttenden
Address: 4600 Campus Drive, Suite 101
Newport Beach, CA 92660
Telephone: 949-399-5382; Cell: 949-887-2677
E-mail: ccruttenden@netchemistry.com

For County: Name: County of Orange HCA/Procurement and Contract Services
Attention: Roland Tabangin
Address: 200 W. Santa Ana Blvd Suite 650
Santa Ana, CA 92701
Telephone: (714) 834-3151
E-mail: rtabangin@ochca.com

CC: Name: County of Orange HCA/PH Community Nursing
Attention: Pat Orme
Address: 1725 W. 17th St., Bldg 50
Santa Ana CA 92706-2316
Telephone: 714-934-7799
E-mail: porme@ochca.com

21. **Precedence:** The Contract documents consist of this Contract and its Attachment and Exhibits. In the event of a conflict between or among 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.

22. **Termination – Orderly:** After receipt of a termination notice from the County of Orange, the Contractor may submit to the County a termination claim, if applicable. Such claim shall be submitted promptly, but in no event later than 60 days from the effective date of the termination, unless one or more extensions in writing are granted by the County upon written request of the Contractor. Upon termination County agrees to pay the Contractor for all services performed prior to termination which meet the requirements of the Contract, provided, however, that such compensation combined with 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 performance of the Contract.

23. **Usage:** No guarantee is given by the County to the Contractor regarding usage of this Contract. Usage figures, if provided, are approximations. The Contractor agrees to supply services and/or commodities requested, as needed by the County of Orange, at rates/prices listed in the Contract, regardless of quantity requested.

24. **Usage Reports:** The Contractor shall submit usage reports on an annual basis to the assigned Deputy Purchasing Agent of the County of Orange user agency/department. The usage report shall be in a format specified by the user agency/department and shall be submitted 90 days prior to the expiration date of the contract term, or any subsequent renewal term, if applicable.

25. **Contractor Screening:** Throughout the term of this Contract, Contractor shall not be listed on any state or federal exclusionary rosters, listed below. County may screen Contractor on a monthly basis to ensure Contractor is not listed on the exclusionary rosters, listed below. If Contractor or its employee(s) are found to be included on any of the rosters indicated below, Contractor shall be deemed in default of its obligation under this Paragraph and shall constitute a cause for County to exercise its right to terminate this Contract immediately. County, in its sole discretion, may afford Contractor an opportunity to cure said default within a reasonable time.

a. United States Department of Health and Human Services, Office of Inspector General (OIG) List of Excluded Individuals & Entities (LEIE) (http://exclusions.oig.hhs.gov).

b. General Services Administration (GSA) System for Award Management (SAM) Excluded Parties List (http://sam.gov).

c. State of California Department of Health Care Services Medi-Cal Suspended and Ineligible Provider List (County Health Care Agency Internal Database).

26. **Debarment:** To the extent applicable, Contractor shall certify in writing that neither Contractor nor its employee(s) are presently debarred, proposed for debarment, declared ineligible or voluntarily excluded from participation in a contractual transaction by any state or federal department or agency. Where Contractor is unable to certify to any of the statements in the written certification, Contractor must include a written explanation thereon for the County to consider. County shall have the right to refuse to enter into this Contract with the Contractor, or terminate this Contract if already entered into, if Contractor either fails to certify or certifies that it is subject of any debarment, pending debarment, declared ineligibility or voluntary exclusion from participation by any state or federal department or agency.

27. **Lobbying:** On the best information and belief, Contractor certifies no federal appropriated funds have been paid or will be paid by, or on behalf of, the Contractor to any person 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 contract.

28. **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.

29. **Gratuities:** The Contractor warrants that no gratuities, in the form of entertainment, gifts or otherwise, were offered or given by the Contractor or any agent or representative of the Contractor to any officer or employee of the 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, the County shall have the right to terminate the Contract, either in whole or in part, and any loss or damage sustained by the County in procuring on the open market any goods or services which the Contractor agreed to supply shall be borne and paid for by the Contractor. The rights and remedies of the 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.

30. **Parking for Delivery Services:** County shall not provide free parking for delivery services.

31. **Software – Protection:** County agrees that all material appropriately marked or identified as proprietary, whether oral or written, and furnished hereunder are provided for County's exclusive use for the purposes of this Contract only and shall be held in confidence. All 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 use, copying, modification and protection and security of licensed programs and optional materials.

32. **Software – Maintenance:** The correction of any residual errors in any software products which may be discovered by Contractor or by County shall be considered maintenance. Such maintenance shall be performed by Contractor without additional charge for the duration of this Contract. Suspected errors discovered by County in the software products shall be handled by the following procedure:

    a. A listing of the output and a copy of the evidential input data in machine-readable format shall be submitted to Contractor along with a completed copy of the appropriate Contractor information form and, if appropriate, a listing of the contents of the memory of the CPU at the time the error was noted.

    b. Errors in the software product as verified by Contractor shall be corrected by providing a new copy of said software product or a new copy of the affected portions in machine-readable format.

    Contractor shall be available to assist County in isolating and correcting error conditions caused by County's particular hardware or operating system at rates specified in this Contract. If Contractor is called upon by the state to correct an error caused by County's negligence, modification by County, County-supplied data, or machine or operator failure or due to any other cause not inherent in the original software products, Contractor reserves the right to charge County for such service on a time and material basis at rates in accordance with the Contract.

33. **Software License:** Contractor hereby grants to County of Orange and County accepts from Contractor, subject to the terms and conditions of this Contract, a non-exclusive, non-

transferable license to use the software products list in this Contract, hereinafter referred to as "software products." The license granted above authorizes County to use the software products in machine-readable form on a single computer system, designated in writing by County to Contractor, provided that if the designated CPU is inoperative due to malfunction, license herein granted shall be temporarily extended to authorize County to use the software products in machine-readable form on any other County CPU until the designated CPU is returned to operation. By prior written notice to Contractor, County may re-designate the CPU in which the software products are to be used and must do so if the re-designation is permanent.

When encryption/CPU ID authorization codes are required to operate the software products, Contractor shall provide all codes to County with shipment of the software. In the case of an inoperative CPU, as defined above, Contractor shall provide a temporary encryption/CPU ID authorization code to County for use on a temporarily authorized CPU until the designated CPU is returned to operation. When changes in designated CPUs occur, Contractor shall issue to County within twenty four (24) hours of notification a temporary encryption/ID authorization code for use on the newly designated CPU until such time a permanent code is assigned.

34. **Software Installation:** The installation date for the software products shall be established in accordance with the provisions below:

a. If County elects to install the software products, County shall have thirty (30) days from the date of receipt of the software products to initially install and evaluate the software. The date of expiration of this period shall hereafter be known as the "installation date." Contractor shall be responsible for providing criteria and test data necessary to check out the software products.
b. If installation by Contractor is required by County, Contractor shall have up to thirty (30) days from the effective date of this Contract to provide initial installation and evaluation of the software products on County's designated CPU. Contractor shall issue written notice of the fact that the software products are operational, and the date of said notice shall be known as the "installation date." It shall be at Contractor's discretion to determine the criteria and tests necessary to allow Contractor to issue a notice to the effect that the system is operational.

County agrees to provide such access to its computer system as may be required by Contractor to properly install and test the software products. County further agrees to provide, at no cost to Contractor, systems and production support as may be required by Contractor during installation.

If installation by Contractor is required by County, Contractor shall provide such installation on County's equipment at the rates specified in this Contract.

35. **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.

36. **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.

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.

Contractor further agrees that County may reproduce such manuals for its own use in maintaining the equipment or software provided hereunder. County agrees to include Contractor's copyright notice on any such documentation reproduced in accordance with copyright instructions to be provided by Contractor.

37. **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.

38. **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 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 and 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. Such reviews and testing shall ensure compliance with all pertinent County security standards as well as any HCA/Environmental Health requirements such as federal tax requirements or HIPAA.

(SIGNATURE PAGE FOLLOWS)

SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties hereto have executed this Contract No. MA-042-21010462 the date set forth opposite their signatures. If the company is a corporation, Contractor shall provide two signatures as follows: 1) the first signature must be either the Chairman of the Board, President, or any Vice President; 2) the second signature must be that of the Secretary, an Assistant Secretary, the Chief Financial Officer, or any Assistant Treasurer. In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution or by-laws demonstrating the legal authority of the signature to bind the company.

Contractor: NetChemistry, Inc.

Chris Cruttenden	PRESIDENT
Print Name	Title
DocuSigned by: Chris Cruttenden 12B8CD443F1640D...	10/9/2020
Signature	Date
Ed Meador	SECRETARY
Print Name	Title
DocuSigned by: Ed Meador 754A4C71EDA64A7...	10/9/2020
Signature	Date

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

Purchasing Agent/Designee Authorized Signature:

Print Name	Title
Signature	Date

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

Brittany E. Mclean	Deputy County Counsel
Print Name	Title
DocuSigned by: Brittany E. Mclean 9713A4061D4343D...	10/13/2020
Signature	Date

ATTACHMENT A

SCOPE OF WORK

A. Background

The Orange County Health Care Agency (OCHCA) Community and Nursing Services Division (CNSD) provides home and community based public health nursing services to OC residents who meet the criteria regardless of financial status. These services consist of Targeted Case Management (TCM), client advocacy, patient referrals, community resource information and health education in a variety of programs that target specific population of:

1. Pregnant and parenting women
2. Children
3. Adults, and older adults

CNSD is responsible for providing over 15,000 public health nursing services to approximately 3,000 individuals annually, the majority being home visits. A comprehensive system is needed to provide effective and efficient solutions along with robust system capabilities.

B. Objective

To implement an integrated, secure and scalable web-based nursing case management system solution to support CNSD in conducting a continuum of public health nurse services, effectively, efficiently and support any applicable compliance regulations and requirements.

C. Overall System Capability

The system must support all functional activities of a nurse case management system including the ability to create internal business workflows, capture demographic information, produce daily work assignment and activity summary sheet and perform audits. The system shall also be capable of managing the following but not limited to:

1. Assessments
2. Nursing notes
3. Care plans
4. Referrals
5. Reports
6. TCM/MAA time surveys

D. Functional Requirements

The system shall have the ability to:

1. View, retrieve and centralize all patient care documents to provide easy access.
2. Monitor CNSD fee-based services using a calendar as a self-tracking tool.
3. Perform electronic documentation of CNSD activities for multiple programs at the individual, family and community level.

4. Create, manage and configure the data fields for CNSD programs within the system, whether they are TCM billable or not.
5. Generate unique identifiers to manage clients and family members comprehensive case management records.
6. Manage billing for comprehensive nurse case management services.
7. Create ad-hoc and customized metrics and have the ability to electronically submit data to the National Family Partnership (NFP) warehouse database if needed.
8. Provide accurate and consistent TCM/Medi-Cal Administrative Activities (MAA) reports for monitoring and reimbursement purposes.
9. Apply role-based access control limiting each identified user role with access to a subset of system functions, pages, tabs, fields and the ability to add, update, delete, or view data.
10. Electronically submit required data and outcomes measures to the Orange County Children and Families Commission as a flat file if needed.
11. Create customizable dashboards to view and manage nursing staff workloads.
12. Provide document manageability (import, export, save and print documents) in all formats.
13. Perform data mining and analytics from system.
14. Interface with the State system to electronically submit TCM claims if needed.
15. Perform search using keywords and other criteria.
16. Create and send email notifications, alerts, and reminders for any activity being performed in the system.
17. Provide and capture an audit trail, status updates of all changes made in the system.
18. Be HIPAA compliant for all tiers required by the County.
19. Create and manage a Time Survey Component. The Time Survey component must produce a daily work assignment and activity summary sheet for all nurses and shall have the ability to perform the following:

    - Edit the daily Time Survey activity sheet
    - Prioritize the Time Survey sheet.
    - Record time spent on general activities, mileage traveling to and from services.
    - Bill by time spent on a service.
    - Bill based on service performed.
    - Capture daily activity of who performed the action against what record, against what program, what kind of action and how long the action took.
    - Compute average time per program and generate a time value based on business rules.
    - Automatically and manually schedule the next activity based on frequency, activity type, activity date, and program factoring in County working days.

E. Non-Functional Requirements

1. The system shall be scalable to accommodate additional users and modules as needed.
2. The system shall comply with regulatory components.
3. The system shall be web-based and have a 99.9% up-time.
4. The system shall be accessible 24 hours a day, 7 days a week.
5. The system shall comply with HCA IT Security requirements.

F. Reports

This system shall have the ability to generate reports for all CNSD programs using a reporting wizard and shall have the ability to:

1. Create canned and ad-hoc reports.
2. Customize reports.
3. Export, print and save reports.
4. Ability to utilize County approved data visualization tools if needed.

G. Technology Requirements

1. The system shall be a Software as a Service model in the cloud accessible to suit HCA CNSD.
2. The system shall have the ability to support all browsers at their current version levels.
3. The system shall have a user login authentication process with SSO if needed.
4. The system shall have a high degree of usability and user-friendliness in terms of navigation, data-entry, reviewing data and running reports.
5. The system shall provide safeguards for referential integrity of all data.
6. All communications must be encrypted in-transit through the use of standard security protocols: SSH, SFTP, SCP, HTTPs. Data at rest must be encrypted.
7. Mobility Requirements:

   - The system shall be device agnostic, i.e., performance shall be identical whether the end user is connecting from a desktop or a tablet or any mobile device.
   - Menus and forms shall scale to display appropriately on any device, regardless of screen resolution, aspect ratio, or orientation.
   - The system shall be designed for optimal performance over slower or unreliable connections.
   - The system shall be designed as the primary expected input methods through the use of drop-down lists, and context-specific fields.

H. Project Management

1. Contractor shall provide a Project Charter and a consolidated Project Plan to County for approval, after being awarded the contract, which identifies all Contractor and HCA tasks and responsibilities. The approved project plan shall be the basis for all project activities, and can be amended in accordance with Contractor and HCA agreed upon change management process. The execution of the project tasks and activities shall be completed using an Agile approach.

2. Contractor and HCA shall be responsible for establishing an organization to manage and deliver the services defined in this Scope of Work. After being awarded the Contract, Contractor shall provide a project organization chart describing the project charter which shall be in place for the duration of this contract. Contractor shall designate a Contractor Project Manager who shall have the authority to commit Contractor resources necessary to satisfy all contractual requirements.

3. Contractor shall identify all relevant assumptions made in the development of the project charter and the project plan, and upon which the estimates have been calculated must be clearly documented.

4. Change management – Contractor shall include a description of the change control management process that will be used in order to manage changes either requested by the County or mitigate any deviation from the plan.

5. Contractor shall develop performance metrics and deliver monthly written project status reports summarizing key activities, comparing plan vs actual and identifying any issues and provide 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 can increase during times where additional communication is needed or required.

6. Contractor shall utilize a comprehensive methodology for ongoing project risk management which addresses such issues as technical risk, resource issues, scheduling problems, and HCA readiness. Contractor shall define escalation procedures to address extended and unresolved problems to County Project Manager. Notification and emergency procedures shall be established in the event of system failure. The escalation procedures shall require approval of County Project Manager. The escalation procedures shall include, but not be limited to the following:

   - Conditions warranting changes to the core team or requiring additional resources in meeting the milestones and/or resolving a problem/issue
   - Time durations between escalating to next level of support
   - A diagram depicting the various levels of response
   - The names, titles, and phone numbers of Contractor personnel responsible for response at the various levels of support

7. Contractor shalll make available, via secure FTP (SFTP), an unencrypted full Production backup from the first of every month, in MS SQL file format or XML (SQL preferred), of all county data, related metadata and associated database schema

I. Development, Testing & Training Environments

Contractor shall develop separate development, testing, and training environments for the system accessible to HCA IT staff. The project stakeholders shall also have access to these environments for monitoring Contractor work, and performing validation. Contractor shall provide a detailed training plan to the County which must be approved by the County project manager.

J. Support and Maintenance Procedures

Contractor shall be responsible for establishing support and maintenance procedures for the SAAS system. Contractor shall provide all necessary documentation and procedures needed to support HCA’s use of the system on a 24/7 basis. Contractor shall follow standard multi-tier support framework in terms of classifying and resolving issues based on severity and mutually acceptable service level expectations. The training shall be broken down into four (4) major groups: End User, Super User, Service Desk/Field Support, Administrator and Software Support.

- End Users

  End Users are the largest group in need of training. They could be further broken down into more specific groups based upon their job function.

- Super User

  A “Super User” will be a staff member that will assist other users with general computer and system problems and will be able to generally distinguish between hardware, operating system, network, and system errors.

- Service Desk/Field Support

  Service Desk/Field Support staff shall be trained at the Super User level and be able to accurately triage and record issues for escalation to higher levels of support, identify issues within the system as well and troubleshoot issues with bar code printers and scanners. Service Desk staff shall also have rights to create and maintain user accounts.

- Administrative Staff

  Administrator staff shall be trained to support the front and back end issues, generate reports and manage the database.

- Software Support

  Software Support staff shall be trained at the level of both super user and service desk staff in addition to some selected aspects of the administrative level training. Software Support shall be charged with testing of new releases and updates.

K. User Acceptance Testing

Contractor in junction with the HCA project team shall develop test scripts consistent with the requirements as described in the SOW. Contractor shall work with the project team to 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 it. HCA users shall assist in the actual test and shall be responsible for final approval of user acceptance test recommendations.

No material adjustments made to the Scope of Work will be authorized without prior written approval of the County. Non-material adjustments may be made with the written approval of the County assigned Deputy Purchasing Agent.

ATTACHMENT B

CONTRACTOR'S SCOPE OF WORK

Proposal Synopsis

Our objective through the following narrative is to demonstrate that NetChemistry has the existing solution, direct experience and qualifications to achieve The County of Orange Health Care Agency (OCHCA) Community Nursing Services Division's (CNSD) request for a Nurse Case Management System (NCMS). We will show how our solution incorporates Targeted Case Management (TCM), client advocacy, patient referrals, community resource information and health education in a variety of modules that can accommodate multiple programs targeting specific populations of: Pregnant, parenting women, children, adults, and older adults.

NetChemistry's Nurse Case Management System meets the overall required system capabilities:

- Daily work assignment
- Activity summary sheet
- Audits
- Assessments
- Nursing notes
- Care plans
- Referrals
- Reports
- HIPAA compliant

Scope of Work

Background/Functional Requirements

NetChemistry has developed a web-based, referral and case management tracking and outcomes system that provides the ability for a provider or network of providers to coordinate client-centered care for individuals, prenatal and postpartum mothers, children and their families with the ability to track services and outcomes. The data system includes the following features which provide a robust environment for tracking prevention and intervention activities: multi-level permissions, multiple agency (provider)/program data silos to protect client confidentiality, web-based referral, confidential case conferencing, service documentation, need/referral status tracking, supervisor oversight, and aggregate outcome reporting. The system passes HIPAA security compliance audits and was awarded the Groundworks Group Creativity Award for Innovative Systems in 2013. Current system functionality meeting requirements of the Scope of Work include the following:

Case Management System Functionality

- Comprehensive case records with unique identifiers
- Electronic documentation of screening, case notes and services
- Individual and family goal planning
- Document upload

- Confidential Peer to Peer communication
- Supervisor-staff management system

Electronic System

- Case assignment, tracking and search capability
- Identifies duplicate referrals (prevents duplicate cases)
- Ability to receive external and internal referrals
- Track user roles and back end audit capabilities

Outcomes

- Care Plan development and documentation
- Tickler system for follow-up and periodic review
- Interactive supervisor review system
- Electronic TCM billing file
- Management and Outcome Reporting

The system is currently being utilized in both Orange and Los Angeles Counties for home visiting-based networks providing prevention and intervention services via both direct electronic referrals from hospital providers and easy data entry for community provider referrals. Additionally, Orange County is developing and tracking encounters for billing Medicaid's Targeted Case Management Program (TCM) through a companion module to the case management system. Detailed features of the current system include the following:

User Permissions – There are no limitations on the number of users assigned. Permission is multilevel with a staff and supervisor level for each agency/program and administrative user access for the network oversight. Users are limited to access cases within their own agency/program or silo; and enhanced security can further limit users to accessing only those cases assigned to them. Users can be identified as TCM billers through the addition of the NPI number to their profile. Administrative users have the ability to assign new user accounts, disable accounts, access administration level aggregate outcome reporting, and address programmatic/system issues through the support ticketing system. They have access to the Staging site which is a replica of the live site for testing. Administrators may only see case level information through a direct link in the support ticketing system. Restrictions on how long a user can remain active on the system without logging on as well password format requirements and timeline for password updates is client driven.

Search Features – Search features with multiple filtering allow users to search for cases on the system by client name, date of birth, staff assigned to the case, by referral source, case Id and case status. User permissions offer users the ability to search for clients within their own agency or by case assignment.

Inbox – Landing page after login for user which includes a list of new cases which for staff level users are those supervisors have assigned and for supervisor level users those which have been referred and are awaiting review and assignment. There is also an inbox for any messages from the internal messaging system. The inbox also is the place for any ticklers/reminders built into the system such as those for TCM requirements.

Online Program Referrals – Ability to receive and send web-based, confidential referrals to request services of agencies via the data system for those on the system.
Confidential messaging is available for two-way conversation between referral party and recipient. Mechanism for recipient to accept, deny or redirect referral gives the agency supervisor discretion to manage agency caseloads.

Case Assignment/Waitlist – Supervisor level user utilizes case assignment capabilities by either using a random assignment mechanism or can select specific staff for assignment. There is a waitlist which can utilized as per their agency/program's policies and procedures. Cases can be generated by online program referral or initiated by a case setup wizard. All new cases receive a system duplication check to ensure client doesn't already exist in the system. Historical cases can be attached to current case without disrupting historical case data.

Demographics/Family Information – A wizard guides user to add information on each family member in the system. The **Intake Form** can be customized for agency/program need. Family is organized under one individual, usually the primary caregiver, and the system can designate a family member which makes them eligible for service. Other children and family members can be added as per agency/program needs to collect information on demographics and subsequent services. Designation of family members (i.e., primary caregiver, target child, child in program) ties to underlying logic to pull information regarding services and activities to be pulled into aggregate outcome reporting. A case information tab is included which lists primary caregiver or client, demographic information, referral source, case status, and place to upload authorization forms and other pertinent case documents, and status of screenings/assessments. Also included is the place for the user to document case notes. The family tab summarizes family members and pertinent information is available for quick reference and can be used to update family information. The family tab allows the user to designate a family member as a TCM client thus initiating functionality for care plan documentation and billing.

Service Planning – A Family Goal Plan allowing for long- and short-term goal setting; identification of family strengths and challenges; logging of activities and referrals including need, provider, and referral status; and update goal status. An **End of Service** log contains information that is utilized to generate aggregate outcome reporting based on the agency's contracted services, approved end of service client assessments and evaluation of progress to be noted.

Visits – Curriculum prescribed visits including intake assessments are currently in the system with data collection on items such as health, early literacy, home safety and community resources being utilized. Intake assessments include demographic items such as income, employment and education status, language spoken, and marital status. Specific health items include immunization status, emergency room visits/reasons, well-baby visit status, health home, insurance coverage and birth outcomes. Visits can be customized.

In Network Referrals – The ability for agencies/program within a network on the case management system have the ability to refer to one another. Different from an initial referral for service, this enables an agency to call on the expertise of another agency in the network to work collaboratively on a case or to hand off a case to a program better equipped to meet the client needs. For example, a community nursing visit for a mother and newborn uncovers a pregnant teen in the family who is eligible and could benefit from the Nurse-Family Partnership® services.

Program Evaluation – As with most funded platforms there are client evaluations used to determine the effectiveness of services. The case management system has tab to insert these evaluations. Dependent on the program design and resources, client evaluation information is provided to the funder either through an annual export or stored in a server for use with a desktop publishing tool.

Aggregate Reporting – Supervisor level users have access to reports for their own agency programs. Reports available include information on referrals and their origins; case status; program outcomes; and evidence-based assessments. Supervisors level users have the ability to click on totals in reports to see report details in order to have more control over quality assurance of data. Administrative level reports give similar information but across agency/program for the network and in an aggregate format with no ability to see the underlying client level information. Reports are modified for the program.

Resource Area – Administrative level users have a content area available to upload forms such as user authorization forms, program specific forms, authorization forms, user manuals, and policies & procedures documents. Through this area also lies the ability to send out notifications and messages to users on the system. Individual agencies/program have a resource tab they can utilize to store agency/program specific forms and a template to store frequently used messages such as those sent to referring agencies to notify referral acceptance.

Confidential support ticketing system –Allows users (staff and supervisors) to submit questions and requests for support which are reviewed by the administrative oversight. Screenshots and documents can be uploaded to the support ticket as well as specific case information enabling support staff to view what user is viewing so issues can be resolved quickly. Tickets can be categorized by support type and urgency; issues requiring technical engineer support can be elevated and messaging within the system keeps a history of issues and fixes. The administrator can track commonalities among tickets and requests, informing policies and practices which can be implemented across the initiative.

Reporting -- The system has a number of tools to assist in managing, tracking and reporting. A number of the reports can be customized to meet the needs of the CNSD. **Management Tools** are available for both supervisor and staff users to assist in managing day-to-day work. Staff have their own worklists to assist them in prioritizing their caseload and a set of ticklers reminding when major milestones have lapsed for a case such as Intake incomplete, no family goal plan. Supervisors can view cases of their staff including the number of cases assigned to each; current case status such as assigned, open, closed, waitlisted; and ability to manage assignment workflow by turning staff on and off for case assignment. The **Supervisor Tab** allows a supervisor to review both visits and cases of those staff assigned to them. Supervisors can easily see open cases by client name and date of birth. Quality assurance flags alert supervisors of issues with individual cases such as those late for visitation or missing goal planning. Informational flagging for cases to track such as elevated risk as per an assessment or missing an important health outcome assist with supervision. The supervisor can utilize this tab as a way to easily view cases ready for supervisor review listed Existing reports.

Table 1: NetChemistry System Reports

Report Name	User	Description	Filter(s)
System Summary	Administrator	Month by month view of key performance metrics: # of cases created/closed, referrals submitted/accepted, secure messages exchanged, screenings performed.	Year

Agency Referral	Administrator	Unique counts of each agency/program referral (from whom/to whom) to provide oversight of where clients are originating.	Month/Year
Agency Status	Administrator	Breaks down by Agency/Program: Caseload of each agency/program by the status (New, Currently Open, Closed, etc) and the distribution outcome reasons.	Month/Year
Goal Report	Administrator	Reports major milestones (outcomes) and services provided by agency/program. Most commonly utilized for a standardized funded service.	Month/Year
Referral Matrix	Supervisor	Provides program/agency unique counts of referrals by agency for service by month.	Year
Goal Report	Supervisor	Reports major milestones (outcomes) and services provided by agency/program. Most commonly utilized for a standardized funded service.	Month/Year Staff
Caseload Report	Supervisor	Provides an up-to-date view of agency/program caseload status by month.	Year

In addition to the standard library of reports, the case management platform has an optional report module that provides the administrators with a reporting server. Users would be allowed to connect to the server and build their own reports and perform their own analysis. During the requirements phase NetChemistry will work with the client to identify reporting needs and develop data sources that can be queried by the client.

The reporting server allows the client to run reports across multiple agencies/programs to report outcomes at the program level but also offers the option to drill down to individual data elements to identify trends and nuances in the program. Data is typically refreshed on a daily basis but can be adjusted based on client needs. This type of reporting is currently being utilized with First 5 LA home visiting programs who are able to provide data reporting on evidence-based home visiting programs, Healthy Families America and Parents as Teachers.

Screening/Assessments -- The NetChemistry system currently has the ability for users to document outcomes on the following assessments/screening tools:

- Ages and Stages Questionnaire-3
- Ages and Stages Questionnaire:SE-2
- Bridges Screening Tool (Orange and LA County versions)

- CHEERS
- Depression, Anxiety and Stress Scale (DASS-21)
- Eyberg Child Behavior Inventory (ECBI)
- Family Experiences: Strengths and Stressors
- Family Stress Checklist
- Keys to Interactive Parenting Scale (KIPS)
- Life Skills Progression (LSP)
- Parent Assessment of Protective Factors (PAPF)
- Parenting Experience Survey
- Parenting Task Checklist
- PHQ 9
- Relationship Assessment Tool

A **Case Summary Tab** shows a complete list of the tools and their status for each individual in the family designated for services. The tool will show with the appropriate administration intervals (6 mos., 12 mos.) and will show the due date and/or if it has been completed/missed. For some tools baseline scores will be displayed.

There is also a place in the system for client evaluation and currently in place are evaluation intake, exit and service outcomes for First 5 OC Children’s and Families Commission.

Targeted Case Management -- A module for documenting, reviewing and the download of a billing file of encounters for Targeted Case Management (TCM) is available and currently being utilized in Orange County by home visiting agencies. Users are identified as TCM billers through entry of their NPI numbers when their account is set up in the system and can be modified to turn them on or off as TCM billers during their time with the agency. The module and the TCM care plan currently in use was approved by the County of Orange LGA and each agency has a billing file customized with their billing identifiers. The module follows the workflow as prescribed by State regulations on setting up a new care plan, documenting encounters, providing periodic review, component code logic, and billing file layout. Each encounter follows four steps: entering visit information; assessing goals and needs; referral follow-up/periodic review; and assignment of component codes. There is a confidential messaging component for supervisor-staff communication regarding encounter review and ticklers built in to keep staff on track for referral status updates and periodic reviews. Clients eligible for TCM services are identified in the case record and information such as name, birthdate and Medi-Cal numbers pull forward into the module.

The **TCM Encounter Log** provides a list of encounters that have been entered into the system and can be sorted by those needing review, waiting for information, ready for billing, or plans needing follow up. This list can be filtered by date range, visit type and/or staff assigned. When using the encounter log the supervisor can message staff on issues that need to be resolved before an encounter can be deemed eligible for billing, see where there are issues by system flagging, and designate encounters as billable or not billable. Encounters to be billed can be done so as a group or can be hand selected by the supervisor. The system will provide a billing file which can then be downloaded and uploaded by staff into the State system.

The NetChemistry system is designed to provide a solution to the case management, tracking and outcome needs required of multiple programs under CNSD. The current NetChemistry case management system features and functions would match the needs outlined in the current RFP. Table 2 compares the functional requirements of the NCMS against current NetChemistry features with notation where customizations are needed:

Table 2: **NCMS Requirements vs NetChemistry Features**

NCMS Functional Requirements	istry Current System Features	Customizations
View, retrieve and centralize all patient care documents to provide easy access.	Currently available. Patient care documents available as designated by user access/program.	Customized to add CNSD programs.
Monitor CNSD fee-based services using calendar as a self- tracking tool.	Currently use ticklers and flags as reminders for TCM activities.	Customized to meet needs of CNSD programs.
Perform electronic documentation of CNSD activities for multiple programs at the individual, family and community level.	Unlimited user access for staff and supervisor. Multiple programs organized in individual data silos to protect data integrity and confidentiality. Visits track individual, family and community level outcomes.	Add initiative name and logo changes; individual program names on reports. Customize to meet needs of CNSD programs / Adjust goal reporting.
Create, manage and configure the data fields for CNSD programs within the system whether they are TCM billable or not.	TCM care plan module integrated but separate from other data fields and are created, managed, configured by NetChemistry engineers in conference with client.	Customize to meet needs of CNSD programs.
Generate unique identifiers to manage clients and family members; comprehensive case management records.	Currently available. Unique identifiers for case, client, family members, visits, encounters.	None anticipated
Manage billing for comprehensive nurse case management services	TCM Module currently has a download feature for State TCM billing.	Customize with OCHCA State TCM billing identifier.

Create ad-hoc and customized metrics and have the ability to electronically submit data to the National Family Partnership (NFP) warehouse database as needed.	Currently provide this service to other clients by hosting data on server for reporting. Being utilized for other evidence-based home visiting programs	Customization to meet the needs of NFP including adding any data collection points not already available in the system.
Provide accurate and consistent TCM/Medi-Cal Administrative Activities (MAA) reports for monitoring and reimbursement purposes.	Currently provide fully functioning TCM Module for care plan development, encounter documentation and billing.	Customize any TCM care plan items; add user NPI numbers; add agency information to billing file. Build MAA monitoring and reimbursement module

NCMS Functional Requirements	NetChemistry Current System Features	Customizations
Apply role-based access control limiting each identified user role with access to a subset of system functions, pages, tabs, fields, and the ability to add, update, delete or view data.	Currently available	None anticipated
Electronically submit required data and outcomes measures to the Orange County Children and Families Commission as a flat file if needed.	Currently provide this functionality to other Commission-funded programs.	Customize file to meet program needs and permissions to release data.
Create customizable dashboards to view and mange nursing staff workloads.	Currently provide this functionality through caseload management tools.	Customize to meet program needs.
Provide document manageability (import, export, save and print documents) in all formats	Currently provide document uploads to case on the case tab; program documents can be uploaded, downloaded in the content area. Standard reports download in CSV format which can then be exported to excel.	None anticipated
Perform data mining and analytics from the system	Currently provide this service to other clients by hosting data on server for reporting.	Customize for program needs.
Interface with the State system to electronically submit TCM	Currently provide this functionality to other OC programs.	Customize by adding user NPI#s; add

claims if needed.		agency information to billing file.
Perform search using keywords and other criteria	Users can search for cases on the system by client name, date of birth, staff assigned to the case, referral source, case Id and case status.	None anticipated
Create and send email notifications, alerts, and reminders for any activity being performed on the system.	User-wide emails/notifications can be sent by an Administrative user through the content area. Alerts and reminders, particularly for TCM care plans, utilize tickers and flags seen in the user's Inbox.	Customize for program needs.

NCMS Functional Requirements	NetChemistry Current System Features	Customizations
Provide and capture an audit trail, status updates of all changes made in the system.	System provides date/time stamps to capture user activity on the system backend which is utilized in researching support tickets/issues. System updates are captured as history in the system by way of versioning; Requirement documents are prepared to outline any changes to the system which are signed and dated by client. Release notes are prepared and sent out to client for any change to the system.	None anticipated
Be HIPAA compliant for all tiers required by the county	NetChemistry has its HIPAA HITEC Certification and its Service Organization Control (SOC) 2 Certification. The SOC 2 Report is performed in accordance with AT 101 and based upon the Trust Services Principles, with the ability to test and report on the design (Type I) and operating (Type II) effectiveness of a service organization's controls (just like SOC 1 / SSAE 16). The SOC 2 report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system, as opposed to SOC 1/SSAE 16 which is focused on the financial reporting controls.	None anticipated

Create and manage a Time Survey Component.	Not currently a feature of the system. NetChemistry has a fully written Requirement Document for TCM Time Survey Module ready to go.	Current requirement document can be customized to meet criteria listed by CNSD.

Customization to the NetChemistry system is undertaken in collaboration with the client. Discussion of internal business workflow and review of system capabilities result in a written requirement document specifying the additions, edits and/or customizations needed. Included in the requirement document are screenshots, when available, of how the changes will appear to the user in the system. Upon agreement by the client and after technical review of NetChemistry engineer(s), the requirement document is signed and dated by the client and slated for development. Once completed, changes will be available for client support staff testing in a staging site and, when both client and NetChemistry have agreed development matches agreed upon requirement document, NetChemistry will push to the live user site. NetChemistry provides written release notes for all development.

NCMS Solution

NetChemistry's NCMS Solution is a Software as a Service (SaaS) based model only where all maintenance, support, upgrades, backups, feeds are continually managed over the course of the contract. We offer continuous support services to the client. These services include a Level 2 support desk, ongoing training as necessary, development of client specific documentation, monitoring and reporting, audit reports on the quality of data, impact analysis and comparative trends. Additionally, to ensure successful expansion after deployment we provide continued education and training, workflow analysis, and workflow redesign.

NCMS Data Migration Conversation/Process

NetChemistry has a long history of migrating third party data into our systems. We have over 10 million patient records where we have migrated legacy referral data, eligibility data, assessment data, CCDs, Labs, Pharmacy and specialty Authorizations

Our philosophy in working with third parties has always been to support their preferred format and make the adjustments and conversions on our side whenever possible. This philosophy has enabled us to exchange data with dozens of external entities every day on both a real time and batch basis. These third-party entities include the primary scope of this project (Eligibility, TCM/MMA billing, etc.). The project requirements describe a process where we will receive a flat file containing some type of demographic/address data and additional (yes/no, score, free text) data. This data will be mapped to fields in the NetChemistry database. The data will be imported, and error checking will occur. All our solutions support industry standard interoperability protocols to interface with third-party electronic data repositories as well.

Team Approach

NetChemistry utilizes subject matter teams of trainers, managers, data integrators and engineers that have delivered a multitude of successful and nationally recognized web-based solutions. Every engagement starts with a lead account manager and a dedicated project manager that will manage the communication, timeline, requirements, development and quality assurance associated with a project. The project manager will work with the client to define goals and the key business drivers that support those goals over the. Our project manager will then build the team that can deliver on those goals.

Based on over 19 years' experience developing complex information systems, we have developed an engagement approach that ensures good communication between our clients and ourselves. We break down our approach into four Phases consisting of: Requirements, Gap Analysis, Development and Acceptance.

Implementation is broken into 4 phases:

Phase 1 – Analysis and Requirements Definition

Identify an Organizational Sponsor whose authority encompasses the business areas impacted by the proposed project and can coordinate resources within the client's organization. Once the Organizational Sponsor has been identified, they may choose to delegate day-to-day responsibility to another employee.

NetChemistry will assign a dedicated project manager as coordinator for resources and as a single point of contact.

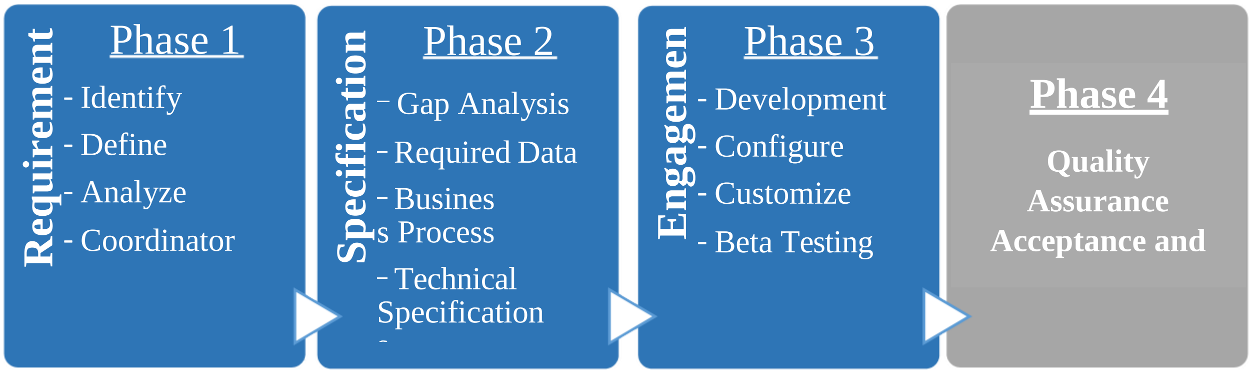
The project manager will work with the client to identify and define requirements and the key business drivers that support project goals. The project manager will coordinate with the Organizational Sponsor to bring together the resources on both sides necessary to develop a complete requirements document based on short and long-term business goals.

Phase 2 – Gap Analysis and Technical Specification

If proposed system uses an existing software system like NetChemistry's case management system, the features of this system will be analyzed and a point by point gap analysis performed. Required data interfaces to be included in the specification will be separated from the application functionality.

The business requirements will then be translated into a technical specification of the deliverables for your proposed information data system. Quality assurance and acceptance criteria are an important component of this specification as they provide an objective method of determining the success of the project.

The technical specification is presented to the client for review and approval. In many cases this is an iterative process in which new requirements may be added or clarified until both parties have a consistent vision of the project.



Requirement

Phase 1

- Identify
- Define
- Analyze
- Coordinator

Specification

Phase 2

- Gap Analysis
- Required Data
- Busines s Process
- Technical Specification
-

Engagemen

Phase 3

- Development
- Configure
- Customize
- Beta Testing

Phase 4

Quality Assurance Acceptance and

System Development

As part of our engagement approach that ensures good communication between our clients and NetChemistry we do not separate out system development from the requirements approach.

Phase 3 – Development and Implementation

1. Configuration of the physical environment: The actual design, coding and hardware installation takes place.

   a) Application - Oracle database install/configuration
   b) Data Warehouse - Oracle database install/configuration
   c) Application software - Implementation of Linux, NetChemistry's Core Product Suite in three environments: Production, Stage and Development.
   d) Customization – (Refer to Scope of Work) Customizations to application(s), business rules, and ata elements
      - Forms Setup
      - Referral Setup
      - Report Center (Data Warehouse) Implementation
      - Initial content population
      - Initial user base population
      - Data exchanges with third party services (Optional)

2. As part of the specification there may be multiple deliverables, each with its own completion date, QA procedures and UAT Plans, i.e., Application Development, Data Warehouse, and Hospital Feeds.
3. During Phase 3 internal testing of the deliverables will take place as part of the normal development process, these are alpha tests.
   a) Setup User Roles
   b) Setup Agencies/Program
   c) Setup Business Rules Regarding type of Referrals
   d) Setup Security

Phase 4 – Quality Assurance and Acceptance

1. Based on the criteria defined in the specification, the completed system is tested first by NetChemistry staff and then in controlled tests with the client. This is the beta test phase.

   a) Setup Test Roles
   b) Draft Testing Scripts based on Functional Requirements & Workflows
   c) User Interface Training
   d) User Interface Training Materials
   e) Report Center Training
   f) Technical Training
   g) Technical Training Materials

h) Issues and Errors logged through Support System

i) Issues and Errors resolved – Support tickets closed

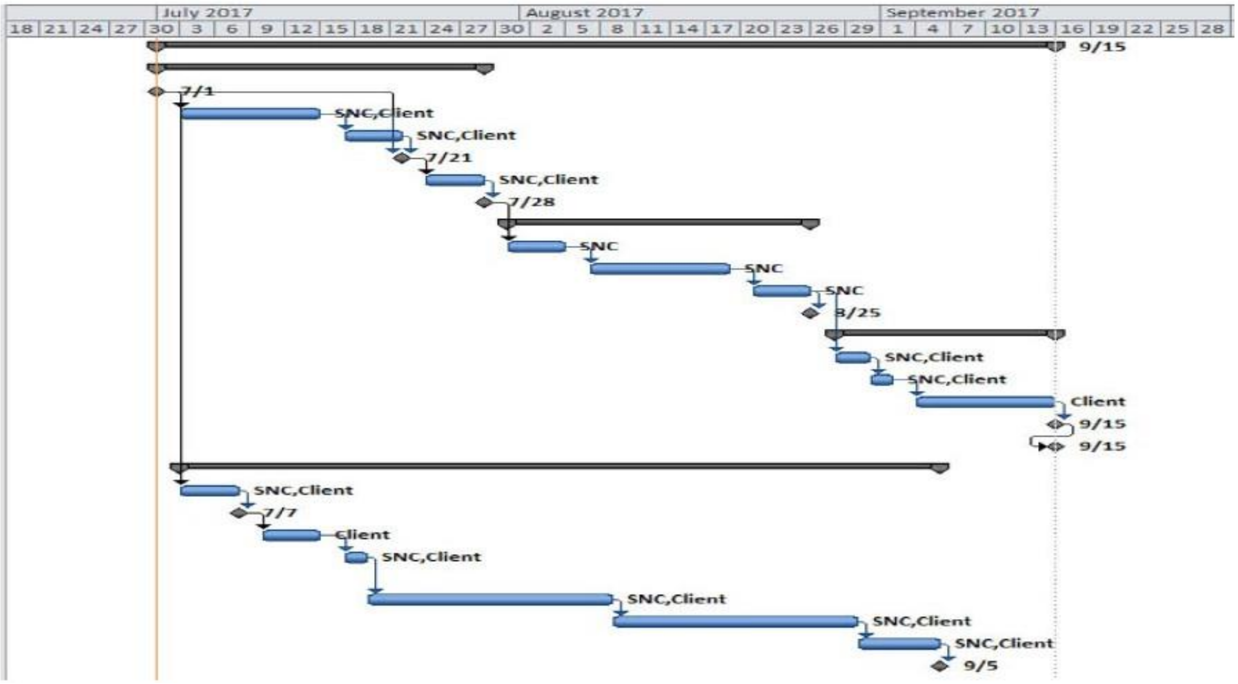
2. After any necessary changes to comply with the specification, the Client performs final User Acceptance Testing.

a) Completion of client and network participant testing

b) UAT sign off by client

c) Live system launch

Proposed implementation timeline – 55 days.



Sample Project Schedule:

Task Name	Duration	Start	Finish	Predecessors	Resource Names
Project Kick Off	**0 days**	**1/23/21**	**1/23/21**		
Contract Sign Off	0 days	1/23/21	1/23/21		Client
Requirements Gathering	**21 days**	**1/23/21**	**2/20/21**		
Review Workflow	3 days	1/23/21	1/25/21	2	NetChemistry, Client
Review Existing Solution	1 day	1/26/21	1/26/21	4	NetChemistry, Client
Review Forms	3 days	1/27/21	1/31/21	5	NetChemistry, Client

Produce GAP Analysis	3 days	2/1/21	2/3/21	6	NetChemistry
Review GAP Analysis	3 days	2/6/21	2/8/21	7	Client
Produce Requirements Document	3 days	2/9/21	2/13/21	8	NetChemistry
Review Requirements Document	5 days	2/14/21	2/20/21	9	Client
Approve Requirements Document	0 days	2/20/21	2/20/21	10	Client
Technical Review	**8 days**	**2/21/21**	**3/2/21**		
Review with Engineering Team	5 days	2/21/21	2/27/21	10	NetChemistry
Provide Timeline for Development	2 days	2/28/21	3/1/21	13	NetChemistry
Schedule Development	1 day	3/2/21	3/2/21	14	NetChemistry
Development Cycle	**45 days**	**3/3/21**	**5/4/21**		
Create Database Back End	2 days	3/3/21	3/6/21	15	NetChemistry
Register/Create Site	1 day	3/7/21	3/7/21	17	NetChemistry
Configure Site	5 days	3/8/21	3/14/21	18	NetChemistry
Systems Development	25 days	3/15/21	4/18/21	19	NetChemistry
Internal QA Testing	5 days	4/19/21	4/25/21	20	NetChemistry
Site Refinement	5 days	4/26/21	5/2/21	21	NetChemistry
Create User Guides	2 days	5/3/21	5/4/21	22	NetChemistry
Push Site to Testing Environment	0 days	5/4/21	5/4/21	23	NetChemistry
Client Testing	**27 days**	**5/5/21**	**6/12/21**		
Client Tests Platform	10 days	5/5/21	5/18/21	24	Client
Client Provides UAT Feedback	2 days	5/19/21	5/22/21	26	Client
NetChemistry Reviews UAT Results	2 days	5/23/21	5/24/21	27	NetChemistry
NetChemistry Fixes any Issues	8 days	5/25/21	6/5/21	28	NetChemistry
Client Does Final Testing	5 days	6/6/21	6/12/21	29	NetChemistry
Client Provides Final Sign Off	0 days	6/12/21	6/12/21	30	Client

Production Push/Go-Live	**2 days**	**6/13/21**	**6/14/21**		
Schedule Production Push	1 day	6/13/21	6/13/21	31	NetChemistry, Client
Push Database	1 day	6/14/21	6/14/21	33	NetChemistry
Push Site to Production Environment	1 day	6/14/21	6/14/21	33	NetChemistry
Notify Client	0 days	6/14/21	6/14/21	35	NetChemistry
Optional Modules	**23 days**	**1/23/21**	**2/22/21**		
Hospital Feed Development	**23 days**	**1/23/21**	**2/22/21**		
Initial Kick Off Call	0 days	1/23/21	1/23/21		NetChemistry, Client, Hospital
Send Hospital IT eCEDA Documentation	1 day	1/23/21	1/23/21	40	NetChemistry
Hospital Sends Cross Reference Tables	5 days	1/24/21	1/30/21	41	Hospital
Hospital Creates Prototype file	10 days	1/24/21	2/6/21	41	Hospital

Licensing Structure

NetChemistry's NCMS is not priced on a per user license or per use basis. NetChemistry offers monthly Service as a Software (SaaS) fee that will allow for up to 25 sites to use the platform on an unlimited basis. All maintenance, support, upgrades, backups, feeds are continually managed over the course of the contract. We offer continuous support services to the client. These services include a Level 2 support desk, ongoing training as necessary, development of client specific documentation, monitoring and reporting, audit reports on quality of NCMS submissions, impact analysis and comparative trends. Additionally, to ensure successful expansion after deployment we provide continued education and training, workflow analysis, and workflow redesign.

Maintenance and Service Structure

NetChemistry's NCMS is a SaaS based model where all data and documentation, technical support, functional upgrades, user support, training, maintenance, backups, data feeds are continually managed over the course of the contract. We offer continuous support services to the client. These services include a Level 2 support desk, ongoing training as necessary, development of client specific documentation, enhancement release notes, monitoring and reporting, audit reports on quality of data submissions, impact analysis and comparative trends. Additionally, to ensure successful expansion after deployment we provide continued education and training, workflow analysis, and workflow redesign. As a standard practice, NetChemistry performs 24/7 maintenance and emergency support of the NCMS system, hardware, server, database software, and connectivity though the SaaS managed hosting model. Security upgrades are proactively installed as needed for the entire system infrastructure during negotiated outage windows. Fixes are included in the ongoing product support and will be provided at no cost. Major software updates are typically available on a 12-month cycle. Availability of minor updates varies. Under the SaaS model, no delivery of updates is required. Updates are visible when logging into the system using a standard web browser.

1. Data and Documentation:

The NetChemistry Professional Services team assigned to the client will collaborate with you to plan and manage implementation and expansion to ensure each unit achieves its goals for successful use of NCMS. The implementation plan will include step by step tasks, resources necessary, and a training plan outline.

NetChemistry utilizes subject matter teams of trainers, managers, data integrators and workflow engineers that have delivered a multitude of successful and nationally recognized web-based solutions. Every engagement starts with a lead account manager and a dedicated project manager that will manage the communication, timeline, requirements, development and quality assurance associated with a project. The project manager will work with the client to define goals and the key business drivers that support those goals.

Once the requirements are completed the Project Management Team will review the requirements with the Engineering team to provide the appropriate timeline/milestone schedule. The Project Plan will then be reviewed with the client and modified based on external factors (reporting deadlines, program deadlines, etc.). Once approved any changes to the Project Plan will need to go through the Change Review Board.

Data migration: The NetChemistry Professional Services team assigned to the client will collaborate with you to plan and manage Data migration and implementation to ensure each unit achieves its goals for successful use of NCMS. The implementation plan includes step-by-step tasks, resources, and a training plan outline.

2. Technical Specifications:

Because our system is SaaS based it can be accessed and used via any device capable of web browsing with internet access. Our standard SLA supports the current web browser version and one previous. We typically support all browser versions currently supported by the client.

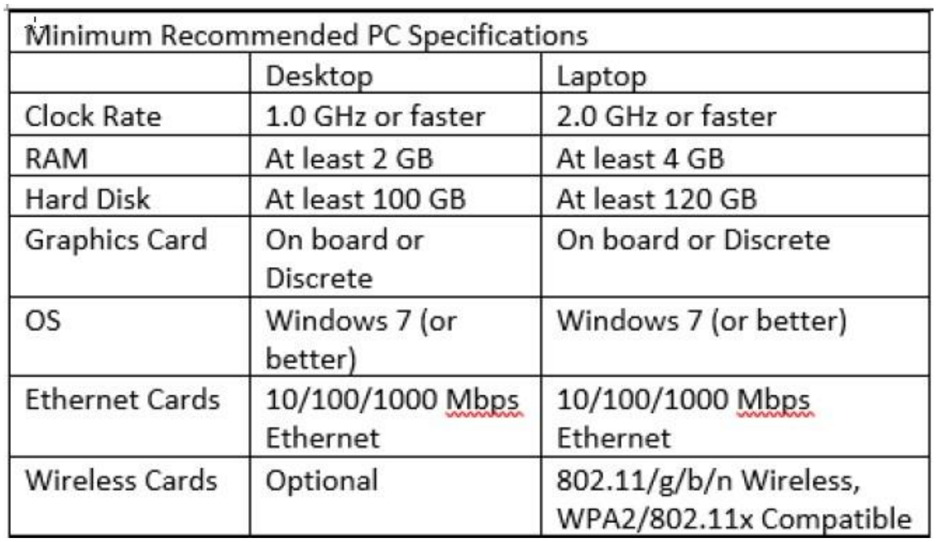
Workstation Device Requirements:

- IE - Current Version or one previous
- Firefox – Current Version or one previous
- Chrome – Current Version or one previous
- Safari – Current Version or one previous

Mobile Device Requirements:

- IE - Current Version or one previous
- Firefox – Current Version or One previous

- Chrome – Current Version or one previous
- Safari – Current Version or one previous



Minimum Recommended PC Specifications		
	Desktop	Laptop
Clock Rate	1.0 GHz or faster	2.0 GHz or faster
RAM	At least 2 GB	At least 4 GB
Hard Disk	At least 100 GB	At least 120 GB
Graphics Card	On board or Discrete	On board or Discrete
OS	Windows 7 (or better)	Windows 7 (or better)
Ethernet Cards	10/100/1000 Mbps Ethernet	10/100/1000 Mbps Ethernet
Wireless Cards	Optional	802.11/g/b/n Wireless, WPA2/802.11x Compatible

3. Functional Requirements:

Based on over 20 years' experience developing complex information systems, we have developed an engagement approach that ensures good communication between our clients and ourselves. We break down our approach into **4 Phases** consisting of: Requirements, Gap Analysis, Development and Acceptance. The use of this process to clearly define the goals and requirements for every engagement continually delivers successful projects as well as happy clients.

Implementation of NCMS is broken into **4 phases**:

– **Phase 1 – Analysis and Requirements Definition** - Gathering requirements, reviewing the platform and the workflow, and identifying any gaps. The project manager will work with the client to identify and define requirements, Data Migration needs and the key business drivers that support project goals. The project manager will coordinate with the Organizational Sponsor to bring together the resources on both sides necessary to develop a complete requirements document based on short and long-term business goals.

– **Phase 2 – Technical Specification System Development** - After finalizing the requirements we establish a development site and engage in any software changes defined in the requirements phase.

– **Phase 3 Engagement and Testing** - Once the changes have been made a Stage environment will be developed to allow the client to test the software. At this point we will train network administrators and testing team who will then engage in the User Acceptance Testing. Upon User Acceptance, the software will be made available in a production environment for use by the end user.

– **Phase 4 – Quality Assurance, Acceptance and Training** - In conjunction with client project leadership, we will meet with program/program staff leadership to provide software demonstration, education, workflow analysis, and workflow redesign as necessary with a focus on patient population, program/program staff organization, and existing program/program staff technology. Additionally, we will complete system configuration including creating program/program staff organizations, specialties, and users. Finally, we will conduct training for all providers and staff at the program/program staff who will be responsible for interacting with the NCMS software.

The first 3 phases of implementation take place over the course of 1 to 2 months, followed by 4 weeks of program/program staff level training depending on the number of program/program staff. Each program/program staff is engaged in 3 meetings over a 3 to 4-weeks.

During Phases 1-3 we provide a project manager, a technical lead, and a software developer. We recommend network level leadership/project administrators, an IT lead, and Referral Workflow Subject Matter Expert (SME). These resources should be familiar with various aspects of software needs, workflow needs, and patient eligibility requirements.

4. Support and Training Requirements:

NetChemistry's NCMS is a SaaS based model where all maintenance, support, upgrades, backups, feeds are continually managed over the course of the contract. We offer continuous support services to the client. These services include a support desk, ongoing training as necessary, development of client specific documentation, enhancement release notes, monitoring and reporting, audit reports on quality of NCMS submissions, impact analysis and comparative trends. Additionally, to ensure successful expansion after deployment we provide continued education and training, workflow analysis, and workflow redesign.

Subscriber Care Support Issue Escalation.

Subscriber Care Hours: NetChemistry technical support business hours are 8 a.m. to 5 p.m., Monday through Friday, Pacific Time. Technical support is closed on all scheduled NetChemistry holidays (generally consistent with all United States federal holidays). Technical support may also be closed because of unforeseen emergencies (e.g., weather conditions, power outages, etc.). In the event of such emergencies, diligent efforts will be made to modify the outgoing voice mail announcement on the telephone support line to provide reason for closure. Emergency issues, limited to the unavailability of NCMS and/or the Site, may be reported 7x24 by calling NetChemistry's Emergency Hotline at (949) 260-9397. NetChemistry's Emergency Hotline phone number is subject to change with 24-hour notice to Subscriber via email.

Issue Escalation: Issues regarding NCMS and/or the Site availability are considered NetChemistry's highest priority. If the issue is deemed to originate with the NCMS and/or the Site hardware or software, the support representative will promptly escalate the issue to NetChemistry's Engineering Group. If NCMS and/or the Site is unavailable for longer than twenty (20) continuous minutes, all affected subscribers will be notified via email to the relevant Use Administrators. Issues regarding general usage, bug reports, documentation, etc., will be handled using the escalation procedure below.

Trouble tickets: are tracked using an integrated multi-level support ticket system. A trouble ticket is generated by the user that includes the time, date, class/severity, and a chronology of the problem as it is managed through a ticket response list. If an issue is deemed to originate with the software application, a support representative can escalate the issue to a Second Level Support request. Issues regarding general usage, bug reports, documentation, etc., will be handled using the escalation procedure below.

First Level Support: is provided via the NCMS system. First Level support is also provided by a specified client support representative and includes answering general service questions via the **integrated support ticket system**. If the issue cannot be answered, it will be escalated to Second Level support.

Second Level Support: consists of senior support representatives and support management; these individuals will make every reasonable attempt to answer the problem during the same business day. Subscriber will be notified by email and informed of the estimated time of resolution. Follow-up messages are sent as deemed necessary to ensure Subscriber is properly informed.

After-hours emergency service line: is used for critical application errors or website unavailable issues. This support consists of senior support representatives; these individuals will make every reasonable attempt to resolve the problem ASAP. Emergency issues, limited to unavailability of the NCMS and/or the Site, may be reported 7x24 (seven days per week; 24 hours per day) by calling NetChemistry's Emergency Hotline at (949) 260-9397. Support by email may also be sent to support@SafetyNetConnect.com.

As a standard practice, NetChemistry performs 24/7 maintenance and emergency support of the hardware, server, database software, and connectivity within every managed hosting agreement. Security upgrades are proactively installed as needed for the entire system infrastructure during negotiated outage windows. Fixes are included in the ongoing product support and will be provided at no cost.

Major software updates are typically available on a 3 to 6-month cycle. Availability of minor updates varies. Under the SaaS model, no delivery of updates is required. Updates are visible when logging into the system using a standard web browser.

NetChemistry technical support business hours are 5 a.m. to 5 p.m. Pacific Time, Monday through Friday. NetChemistry technical support is closed on all scheduled NetChemistry holidays (which are consistent with all United States federal holidays, except as otherwise communicated in writing by NetChemistry to Subscriber). NetChemistry technical support may be closed because of unforeseen emergencies (e.g., weather conditions, power outages, etc.). In the event of such emergencies, NetChemistry will use best efforts to setup an auto-generated email response to emails sent to support@netchemistry.com to provide the reason for closure and the expected date and time for technical support to re-open.

Emergency issues, limited to unavailability of, hacking of or other unauthorized activity involving NCMS and/or the Site and other usage issues involving NCMS and/or the Site that occur outside NetChemistry's normal technical support business hours and are not resolved via online help and FAQ documents located on NCMS and/or the Site, may be reported 7x24 by calling NetChemistry's Emergency Hotline at (949) 644-7050. NetChemistry's Emergency Hotline phone number is subject to change with no less than twenty-four (24) hour advance notice to Subscriber via email to the Account Manager.

Training: During Phase 4 we will provide 1-2 trainers depending on program/program staff size. We recommend Project Administrators as well as program/program staff site leadership be involved in all three implementation meetings in order to adequately address program/program staff needs, behavior, and desired outcomes. They key leadership roles are the CMO, COO, lead nurse, lead case manager/referral manager, and staff manager. Additionally, primary care providers (including NPs, RNs, PAs, etc.) who will submit NCMSs, as well as any staff (including MAs, referral clerks/coordinators, nurses, front office staff) who may assist in the NCMS process of gathering documentation or taking photos will be included in training meetings.

5. Operations and Maintenance Procedures:

Ongoing maintenance: The client will be not be required to perform any maintenance of the solution. We offer continuous support services to the client. These services include a Level 2 support desk, ongoing training as necessary, development of client specific documentation, monitoring and reporting, audit reports on quality of NCMS submissions, impact analysis and comparative trends. Additionally, to ensure successful expansion after deployment we provide continued education, workflow analysis, and workflow redesign.

After 10 years of providing NCMSs and having dealt with the volume NetChemistry has processed through its platform, we know how to ensure continuity and quality. We have been able to build the tools that focus on supporting the oversight and management of the NCMS deployment, provide real-time capability to impact workflow and use evidence-based practices while continually maintaining a focus on improving the care of the patient.

6. Implementation Tasks:

Go-Live: Based on the criteria defined in the specification, the completed system is tested first by NetChemistry staff and then in controlled tests with the client.

- Setup Test Roles and Use case Scripts
- User Interface Training and Materials
- Report Center Training
- Technical Training Materials

After any changes to comply with the specification, the Client performs final User:

- Acceptance Testing.
- Completion of client testing
- UAT sign off by client
- Live system launch (Go- Live)

To ensure successful go-live we begin with education, workflow analysis, and workflow redesign as necessary with a focus on patient population, program/program staff organization, and existing program/program staff technology. We engage in a current-state and future-state workflow discussion with project leadership team regarding the referral and consultation processes supported by NCMS. The Development of workflow illustrations is included.

The Project Management team will establish the appropriate Communication Plan protocols during the initial phases of the project with the business owner. Protocols include:

Change Management Process: The approval process varies by client, but the typical implementation includes a review/approval process that includes a project champion, change review board and the NetChemistry Project Management Team. All changes to the project/platform are review and approved by this team before it is sent to the engineering team for development. This team will be responsible for:

- Prioritization of Issues (During/After Implementation) – based on risk to the workflow
- Review and Approval of Requirements Documents
- Establishment of Timelines/Expectations

Plan for transition: Additionally, to ensure successful expansion after deployment we provide continued education and training, workflow analysis, and workflow redesign. Our training approach is multifaceted and includes not only use of the system but also workflow integration and thus includes users at the network, organization, and program level. We begin by meeting with network leadership to provide education, workflow analysis and redesign as necessary, as well as software demonstrations. We also discuss provider awareness, eligibility, resources and staffing models, and specialty provider responsibilities.

Risk Registry: Throughout the project life cycle a risk registry will be maintained to maintain visibility of issues that may impact the successful implementation of the project. Risks include (but not limited to):

- Program Development Schedules
- Workflow Changes/Issues
- Client Technical resource availability
- Compressed Project Timeline

ATTACHMENT C

COMPENSATION AND INVOICING

1. **Compensation**

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

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

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

See Attachment D – Cost Summary/Pricing

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

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

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

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

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

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

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

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

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

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

Invoice and support documentation are to be forwarded to:

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

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

ATTACHMENT D

COST SUMMARY/PRICING

DISCRIPTION	YEAR 1 COST	YEAR 2 COST	YEAR 3 COST	YEAR 4 COST	YEAR 5 COST
Software Implementation fees	$80,000	$0	$0	$0	$0
Requirements	$60,000	$10,000	$10,000	$10,000	$10,000
Customization	$40,000	$15,000	$15,000	$15,000	$15,000
Establish Data Feeds	$10,000	$0	$0	$0	$0
Training	$20,000	$0	$0	$0	$0
User Manuals					
Data Migration/Conversion	$15,000	$0	$0	$0	$0
System Hardware, Maintenance, and Support Service	$120,000	$120,000	$120,000	$120,000	$120,000
NetChemistry Software License Fee					
Technical Support					
Production and Development Hardware:					
Redundant Database Layer Servers					
Redundant Web Layer Servers					
Raid Storage Layer					
Redundant Power					
Tape Backup Layer					
Firewall Layer					
Redundant DNS Server					
100mbps Burstable Bandwidth					
Encrypted data backup/restore					
Oracle and Veritas software licenses					
24x7 full resolution monitoring staff”					
Colocation at Evoque Data Center Solutions™					
located in Irvine, CA and Lisle, IL					
Security updates and patches					
Soc 2 Audits					
Stage, Training and Production Environments					
Tableau Report Service (Optional)	$15,000	$15,000	$15,000	$15,000	$15,000
Unlimited Users	$0	$0	$0	$0	$0
Unlimited Sites	$0	$0	$0	$0	$0
Annual Cost Total By Year:	$360,000	$160,000	$160,000	$160,000	$160,000

ATTACHMENT E

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:

CONTRACTOR does not promptly enter into negotiations to amend this Business Associate Contract when requested by COUNTY pursuant to this Paragraph C; or

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:

Complying with all of the data system security precautions listed under Paragraphs E, below;

Achieving and maintaining compliance with the HIPAA Security Rule, as necessary in conducting operations on behalf of COUNTY;

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

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

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

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

E. DATA SECURITY REQUIREMENTS

1. Personal Controls

a. Employee Training. All workforce members who assist in the performance of functions or activities on behalf of COUNTY in connection with Agreement, or access or disclose PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY, must complete information privacy and security training, at least annually, at CONTRACTOR's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following the termination of Agreement.

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

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

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

2. Technical Security Controls

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

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

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

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

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

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

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

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

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

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

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

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

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

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

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

3. Audit Controls

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

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

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

4. Business Continuity/Disaster Recovery Control

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

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

5. Paper Document Controls

a. Supervision of Data. PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. Such PHI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

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

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

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

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

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

F. BREACH DISCOVERY AND NOTIFICATION

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

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

b. CONTRACTOR shall be deemed to have knowledge of a Breach, if the Breach is known, or by exercising reasonable diligence would have known, to any person who is an employee, officer, or other agent of CONTRACTOR, as determined by federal common law of agency.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

G. PERMITTED USES AND DISCLOSURES BY CONTRACTOR

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

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

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

i. The Disclosure is required by law; or

ii. CONTRACTOR obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person and the person immediately notifies CONTRACTOR of any instance of which it is aware in which the confidentiality of the information has been breached.

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

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

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

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

H. PROHIBITED USES AND DISCLOSURES

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

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

I. OBLIGATIONS OF COUNTY

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

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

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

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

J. BUSINESS ASSOCIATE TERMINATION

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

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

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

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

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

b. CONTRACTOR shall retain no copies of the PHI.

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

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

Attachment E-1

PERSONAL INFORMATION PRIVACY AND SECURITY CONTRACT

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

A. DEFINITIONS

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

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

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

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

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

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

voice print, a photograph or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper or any other medium.

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

8. "Personal Information" (PI) shall have the meaning given to such term in California Civil Code§ 1798.3(a).

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

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

B. TERMS OF AGREEMENT

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

2. Responsibilities of CONTRACTOR

CONTRACTOR agrees:

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

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

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

i. Complying with all of the data system security precautions listed in Paragraph E of the Business Associate Contract, Attachment 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 beach of unsecured DHCS PI and PII or security incident in accordance with Paragraph F, of the Business Associate Contract, Attachment C to the Agreement.

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

ATTACHMENT F

OCHCA SECURITY REQUIREMENTS AND GUIDELINES FOR CONTRACTORS AND APPLICATION SERVICE PROVIDERS

County of Orange
Health Care Agency

Security Requirements and Guidelines for Application Vendors and Application Service Providers

04/2018

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 Sarbanes- Oxley (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:

- **SSAE 18.** SSAE 18 SOC 2 Type 2 or SOC 3 compliance certificate

- **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.
- **Jurisdiction and Location of OCHCA Data.** To protect against seizure and improper use by non-United States (US) persons and government entities, all data / information stored and processed for OCHCA must reside in a facility under the legal jurisdiction of the US.
- **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 custom- crafted 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:

- OCHCA Security Requirements and Guidelines for Application Vendors and Application Service Providers - Questionnaire
- Business Continuity Plan Summary (as related to service provided)
- SSAE 18 SOC 2 Type 2 or SOC 3 compliance certificate
- Network Diagram that demonstrates vendor network and application segmentation including the security controls in place to protect HCA data
- 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