CONTRACT NO. MA-042-23010683

FOR

MULTI-DRUG RESISTANT ORGANISM (MDRO) DATA EXCHANGE SOFTWARE

BETWEEN

COUNTY OF ORANGE
(HEALTH CARE AGENCY)

AND

ALTARUM INSTITUTE

Table of Contents

CONTRACT NO. MA-042-23010683

FOR

MULTI-DRUG RESISTANT ORGANISM (MDRO) DATA EXCHANGE SOFTWARE

WITH

ALTARUM INSTITUTE

This Contract Number MA-042-23010683 ("Contract") is made and entered into this 8th day of August, 2023 ("Effective Date") between **Altarum Institute** ("Contractor"), with a place of business at 3520 Green Court, Suite 300, Ann Arbor, MI 48105, and County of Orange, a political subdivision of the State of California ("County"), through its Health Care Agency with a place of business at 405 W. 5th Street, Suite 600, 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 incorporated by reference into this Contract and constitute a part of this Contract:

Attachment A – Scope of Work
Attachment B – Compensation and Invoicing
Attachment C – Cost Summary/Pricing
Attachment D – Business Associate Contract
Attachment D-1 – Personal Information Privacy and Security Contract
Attachment E – OCHCA Security Requirements and Guidelines for Vendors and Application Service Providers

Recitals

WHEREAS, County issued a Request for Proposals (RFP) for a **Multi-Drug Resistant Organism (MDRO) Data Exchange Software** and

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

WHEREAS, Contractor agrees to provide the **Multi-Drug Resistant Organism (MDRO) Data Exchange Software** to 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, Contractor agrees to comply with the business associate requirements set forth in the Business Associate Contract, attached hereto as Attachment D; and

WHEREAS, County of Orange Board of Supervisors has authorized County Procurement Officer or designee to enter into a Contract for **Multi-Drug Resistant Organism (MDRO) Data Exchange Software** with 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 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, agreements, or undertakings other than those set forth herein or referred to herein. All previous proposals, offers, discussions, preliminary understandings, and other communications relative to this Contract, oral or written, are hereby superseded, except to the extent that they have been incorporated into this Contract. Further, any other provision or other unilateral terms which may be issued by Contractor before or during the term of this Contract, irrespective of whether any such provisions or terms may be affixed to or accompany the goods and services being purchased, are hereby superseded and are not valid or binding on County unless authorized by County in writing in an amendment to this Contract.

   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 authorized by County in writing in an amendment to this Contract. All automated end-user agreements (including, but not limited to, click-throughs, shrink-wrap, browse wrap and other non-negotiated terms and conditions provided with any of Contractor's services) and documentation provided with any of the services are specifically excluded and null and void. All terms and conditions in such agreements and documentation do not constitute a part or amendment of this Contract and shall have no force and effect and shall be non-binding on County, its employees, agents, and other authorized users, even if access to or use of such service or documentation requires affirmative acceptance of such terms and conditions.

C. **Amendments:** Except as expressly provided herein, no changes, modifications, or amendments to the terms and conditions of this Contract are valid or binding on County unless made in writing and signed by the duly authorized representative of the parties. No other act, document, usage, or custom shall be deemed to change, modify, or amend this Contract. Nor shall any oral understanding or Contract not incorporated herein be binding

on either of the parties; and no exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing.

D. **Taxes:** Unless otherwise provided herein or by law, the price stated in Attachment B 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 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 Scope 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 pursuant to Paragraph F.

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 after County's satisfactory acceptance in accordance with the requirements of Attachment B.

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. All warranties in this Contract shall inure to County, its successors, assigns, customer agencies, and governmental users of the services. Contractor will indemnify, defend and hold County and County Indemnitees, 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 and by reason of 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 is solely responsible for clearing the right to use any patented or copyrighted materials in the performance of this Contract. Contractor warrants that any materials (e.g., software, documentation, specifications) or any part thereof, as modified through services provided under this Contract, will not infringe upon or misappropriate any patent, copyright, trademark, trade secret, or any other proprietary right, of any third party. Contractor agrees that, in accordance with the more specific requirement contained in Paragraph Z, 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 and attorney's fees.

In the event any materials or any part thereof, as modified through the services provided under this Contract, is or becomes the subject of a claim of infringement or misappropriation of a patent, copyright, trademark, trade secret, or any other proprietary right, or is enjoined, Contractor will with all reasonable speed and due diligence provide or otherwise secure for County, at Contractor's expense and election, subject to County approval not to be unreasonably withheld, one of the following: (a) the right to continue use of any such materials or any part thereof to the full extent contemplated by this Contract; (b) an equivalent system having the specifications as provided in this Contract; or (c) modification of the system or its component parts so that they become non-infringing while performing in a substantially similar manner to the original system and meeting the requirements of this Contract. If none of these options are available on commercially reasonable terms, County shall stop using the affected services provided under this Contract and Contractor shall refund to County any sums County paid to Contractor for the affected services, less a reasonable offset for use. County then has the option of immediately terminating the Contract, or applicable portions thereof, without penalty for cause pursuant to Paragraph K, Termination.

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 prior written consent of County. Contractor shall provide County no less than sixty (60) calendar days' written notification of its intent to assign, sell, delegate or otherwise dispose of the rights and obligations of this Contract. Any attempt by Contractor to assign the performance or any portion thereof of this Contract without the express prior written consent of County shall be void and invalid and shall constitute a material 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.

L. **Consent to Breach Not Waiver:** Any action or inaction by County or failure of County in any one or more instances to insist upon strict performance of any of the terms of this Contract or to enforce any right or provision contained herein shall not be construed as a waiver or relinquishment by County of its rights hereunder and shall not prevent County from enforcing such provision or right on any future occasion. Further, no term or provision of this Contract shall be deemed waived and no breach excused, unless such waiver or consent is 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 warrants all work under this Contract, taking necessary steps and precautions to perform the work to County's satisfaction**.** Contractor is responsible for the professional quality, technical assurance, timely completion and coordination of all documentation and other goods/services furnished by 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; and, if permitted to subcontract, Contractor is fully responsible for all work performed by subcontractors.

Contractor further warrants that: a) Contractor has and will continue to have the unconditional and irrevocable right, power, and authority, including all permits and licenses required, to provide the services and to grant all rights and licenses granted or required to be granted by it under this Contract; b) Contractor has not and will not assign or otherwise enter into an Contract Contract by which it purports to assign or transfer any right, title, or interest to any technology or intellectual property right that would conflict with its obligations under this Contract; c) Contractor will and has the expertise to perform all services in a timely, professional and workmanlike manner with a level of care, skill, practice, and judgment consistent with the highest professional standards and with generally recognized industry standards and practices for similar services, using personnel with the requisite skill, experience, and qualifications, and will devote adequate resources to meet Contractor's obligations under this Contract; d) Contractor will use its best efforts to ensure that no harmful code, malware, or similar items are introduced into County's computing and network environment by the services, and that, where such items are transferred to County through the services, Contractor shall reimburse County the actual cost incurred by County to remove or recover from such items, including the costs of persons employed by County; and e) Contractor will not knowingly use the services of any ineligible person or subcontractor for any purpose in the performance of the Services under this Contract.

O. **Insurance Requirements:**

Prior to the provision of services under this Contract, the Contractor agrees to carry 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 current, provide Certificates of Insurance, and endorsements to the County during the entire term of this Contract.

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 SIRs in excess of Fifty Thousand Dollars $50,000 shall specifically be approved by the County's Risk Manager, or designee. The County reserves the right to require current audited financial reports from Contractor. If Contractor is self-insured, Contractor will indemnify the County for any and all claims resulting or arising from Contractor's services in accordance with the indemnity provision stated in this contract.

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).**

If the insurance carrier does not have an A.M. Best Rating of A-/VIII, CEO/ 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

Increased insurance limits may be satisfied with Excess/Umbrella policies. Excess/Umbrella policies when required must provide Follow Form coverage.

Required Coverage Forms

The Commercial General Liability coverage shall be written on occurrence basis utilizing 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-contributory 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-contributory 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 provide thirty (30) days prior written notice to the County of any policy cancellation or non-renewal and ten (10) days prior written notice where cancellation is due to 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 the following:

1) The retroactive date must be shown and must be before the date of the contract or the beginning of the contract services.

2) Insurance must be maintained, and evidence of insurance must be provided for at least three (3) years after expiration or earlier termination of contract services.

3) If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the effective date of the contract services, Contractor must purchase an extended reporting period for a minimum of three (3) years after expiration of earlier termination of the Contract.

The Commercial General Liability policy shall contain a severability of interests clause also known as a "separation of insureds" clause (standard in the ISO CG 0001 policy).

Insurance certificates should be forwarded to the agency/department address listed on the solicitation.

If 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 provide acceptable Certificates of Insurance and endorsements to 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 County's express prior written consent via an amendment.

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 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 County.

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

In addition, Contractor must notify County in writing of any change in Contractor's status with respect to name changes that do not require an assignment of the Contract. Contractor also must notify County in writing if Contractor becomes a party to any litigation against County, or a party to litigation that may reasonably affect 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 must provide this information without prompting from County any time there is a change in Contractor's name, conflict of interest or litigation status, Contractor must also provide an update to County of its status in these areas whenever requested by County.

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 Contractor, this obligation applies to Contractor's employees, agents, and subcontractors associated with the provision of goods and services provided under this Contract. 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 to the extent such delay is caused by any act of God, war, civil disorder, employment strike or other similar cause, beyond Contractor's reasonable control, provided Contractor gives written notice of the cause of the delay to County within thirty-six (36) hours of the start of the delay and Contractor avails itself of any available

remedies to end the delay and minimize the effects of such delay. County may terminate this Contract by written notice to Contractor if the delay continues substantially uninterrupted for a period of five (5) business days or more. No Force Majeure event excuses Contractor's other obligations under this Contract.
Notwithstanding the foregoing or any provision of this Contract, in no event will the following be considered a Force Majeure event: (a) shutdowns, disruptions, or malfunctions of Contractor's systems or any of Contractor's telecommunication or internet services other than as a result of general and widespread internet or telecommunication failures that are not limited to Contractor's systems; and (b) the delay or failure of any Contractor personnel (including subcontractors) to perform any obligation of Contractor hereunder unless such delay or failure to perform is itself by reason of a Force Majeure event.

S. **Confidentiality:**

(1) In the event of a conflict between the provisions of this Paragraph and the provisions of the Business Associate Contract (i.e., Attachment C) and Personal Information Privacy and Security Requirements (i.e., Attachment D), the order of precedence shall be the provisions of the Business Associate Contract and PII Security Requirements and then the requirements of this Paragraph.
(2) All County Data, as defined in Paragraph _ ("County Data"), shall be confidential. Contractor must hold County Data in strict confidence and maintain the privacy and confidentiality of County Data in accordance with and pursuant to all applicable laws relating to privacy and confidentiality that currently exist or may exist at any time during the term of this Contract. Contractor shall protect County Data from unauthorized access, use, disclosure and loss through the observance of the same or more effective procedural requirements as used by County. In addition, Contractor must not use, modify, merge with other data, commercially exploit, make available or make any other use of County Data or take, or refrain from taking, any other action that might, in any manner or form, adversely affect or jeopardize the integrity, security, or confidentiality of County Data, except as expressly permitted in this Contract or as expressly directed by County in writing. Contractor also must not copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose, such County Data to third parties other than employees, agents, or subcontractors who require the County Data for performance of this Contract. The obligation in this Paragraph applies to Contractor's employees, agents and subcontractors.
(3) Contractor must immediately report in accordance with Attachments C and D to County any and all unauthorized disclosures or uses of County Data or suspected or threatened unauthorized disclosures or uses of County Data of which Contractor or Contractor's employees, agents and/or subcontractors are aware or have knowledge or reasonable belief. Contractor acknowledges that any unauthorized publication or disclosure of County Data to others or unauthorized use of County Data may cause immediate and irreparable harm to County. If Contractor should publish, disclose, or use such County Data without authorization, or threaten such action, County is immediately entitled to injunctive relief and any other remedies to which it is entitled under law or equity, without requiring a cure period. Contractor must, in accordance with the more specific requirements contained in Paragraph Z, indemnify, defend, and hold County and County Indemnitees harmless from and against any and all damages, costs, liabilities, and expenses (including without limitation attorneys' fees) relating to or arising from Contractor's unauthorized publication, use, or disclosure of County Data.

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, 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 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 its 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 its own choosing or has knowingly declined to seek such counsel despite being encouraged and given the opportunity to do so. Each party further acknowledges that it has not been influenced to any extent whatsoever in executing this Contract by any other party hereto or by any person representing 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:** Contractor warrants that it is and will remain in full compliance with all Federal and State statutes and regulations regarding the employment of aliens and others and that all its employees performing work under this Contract meet the citizenship or alien status requirement set forth in Federal statutes and regulations. Contractor shall obtain, from all employees performing work hereunder, all verification and other documentation of employment eligibility status required by Federal or State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, 8 U.S.C. §1324 et seq., as they currently exist and as they may be hereafter amended. Contractor shall retain all such documentation for all covered employees for the period prescribed by the law. Contractor shall indemnify, defend with counsel approved in writing by County, and hold harmless, County, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against Contractor or 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 must permit County's Auditor-Controller or the Auditor-Controller's authorized representative (including auditors from a private auditing firm hired by County) access during normal working hours to all books, accounts, records, reports, files, financial records, supporting documentation, including payroll and accounts payable/receivable records, and other papers or property of Contractor for the purpose of auditing or inspecting any aspect of performance under this Contract. The inspection and/or audit will be confined to those matters connected with the performance of the Contract including, but not limited to, the costs of administering the Contract. County will provide reasonable notice of such an audit or inspection.

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

Contractor must maintain such records for possible audit for a minimum of three (3) years after final payment, unless a longer period of records retention is stipulated under this Contract or by law. Contractor agrees to allow interviews of any employees or others who might reasonably have information related to such records. Further, Contractor must include in each subcontract a similar right to County to audit records and interview staff of any subcontractor related to performance of this Contract.

Should Contractor cease to exist as a legal entity, Contractor's records pertaining to this Contract shall be forwarded to County's DPA.

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:** Contractor shall notify the County of Orange assigned Deputy Purchasing Agent in writing when the expenditures against the Contract reach seventy-five percent (75%) of the dollar limit on the Contract. County is not 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 Contractor shall provide **Multi-Drug Resistant Organism (MDRO) Data Exchange Software** to County, as further detailed in Attachment A, Scope of Work.

2. **Term of Contract:** This Contract shall commence on September 23, 2023 through and including September 22, 2026, renewable for two (2) additional years upon agreement of both Parties. Contract shall be in effect for the time periods specified, unless this Contract is terminated earlier by the Parties. Any renewal may require Board of Supervisors' approval. County does not have to give reason if it decides not to renew.

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

   a) Terminate the Contract immediately for cause without penalty pursuant to Paragraph K, Termination;

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

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

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

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

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

   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. County's Project Manager has the right to require the removal and replacement of Contractor's Project Manager and Contractor personnel from providing services to County

under this Contract. County's Project Manager shall notify Contractor in writing of such action. Contractor shall accomplish the removal within five (5) business days after written notice by County's Project Manager. County's Project Manager shall review and approve the appointment of the replacement for Contractor's Project Manager. County is not required to provide any additional information, reason or rationale in the event it requires the removal of Contractor's Project Manager and/or Contractor personnel from providing further services under the Contract.

7. **Contractor's Records:** Contractor shall keep true and accurate accounts, records, books and data which shall correctly reflect the business transacted by Contractor in accordance with generally accepted accounting principles. These records shall be stored in Orange County for a period of three (3) years after final payment is received from County. Storage of records in another county will require written consent from the County of Orange DPA.

8. **Conditions Affecting Work:** Contractor is 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 Contractor to do so will not relieve Contractor from responsibility for successfully performing the work without additional cost to County. 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 during or prior to the execution of this Contract, unless such understanding or representations by County are expressly stated in the Contract and the Contract expressly provides that County assumes the responsibility.

9. **Cooperative Contract:** This Contract is a cooperative contract and may be utilized by all County of Orange departments.

   The provisions and pricing of this Contract will be extended to other governmental entities. Governmental entities wishing to use this Contract will be responsible for issuing their own purchase documents, providing for their own acceptance, and making any subsequent payments. Contractor shall be required to include in any subordinate contract entered into with another governmental entity pursuant to 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. Governmental entities are responsible for obtaining all certificates of insurance, endorsements and bonds required. The Parties agree that any other governmental entity utilizing this Contract shall not be deemed to be an agent or employee of County for any purpose whatsoever. The Contractor is responsible for providing each governmental entity a copy of this Contract upon request. 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 County of Orange departments and governmental 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.

   Subordinate contracts must be executed prior to the expiration or earlier termination of this Contract and may survive the expiration of this Contract up to a maximum of one year; however, in no case shall a subordinate contract exceed five (5) years in duration.

10. **County Data and Ownership:**

(1) All materials, documents, data, reports, information, or any other materials/information that Contractor obtains directly from County or from another entity on behalf of the County from any County data files, databases or medium in the performance of this Contract is owned solely and exclusively by County and shall remain at all times the property of County. Additionally, all materials, documents, data, reports, information, or any other materials that Contractor creates and/or receives in the course of performance of this Contract as relate to the services described in Attachment A, including, but not limited to, personally identifying information (such as demographic data) and/or protected health information, is owned solely and exclusively by County. The foregoing shall constitute for purposes of this Contract and be referred to throughout this Contract as "County Data", and the Parties agree that it shall be liberally construed to include any data or materials that fall within intent and scope of the description above.

(2) County Data may not be used or copied for direct or indirect use by Contractor, except as required in connection with performance of Contractor's duties under this Contract or as specifically directed by County in writing. Contractor must keep and maintain County Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss, and Contractor may not otherwise use, disclose, modify, merge with other data, commercially exploit, make available or make any other use of County Data or take, or refrain from taking, any other action that might, in any manner or form, adversely affect or jeopardize the integrity, security, or confidentiality of County Data, except as expressly permitted herein or as expressly directed by County in writing.

(3) Upon the expiration, earlier termination, or cancelling of this Contract, Contractor shall promptly and without any reasonable delay return and destroy all County Data and shall not retain any copy of the County Data. To the extent the County Data includes materials, documents, data, reports, information, or any other materials/information that Contractor has created and/or received in the course of performance of this Contract as relate to the services described in Attachment A, including, but not limited to, personally identifying information (such as demographic data) and/or protected health information, Contractor shall return or destroy such County Data and shall not retain any copy of such County Data as set forth in more detail in Section H.2 of the Attachment C. To the extent there is any uncertainty as to whether data constitutes County Data, the data in question must be treated as County Data. As between the Parties, County owns all right, title, and interest in, and all intellectual property rights in and to, all County Data. In addition, Contractor shall provide access to and/or a copy of any County Data upon request by the County within a reasonable time under the given circumstances.

(4) In the event of disaster or catastrophic failure that results in significant County Data loss or extended loss of access to County Data or services, Contractor must notify County by fastest means available and in writing, within twenty-four (24) hours after Contractor reasonably believes there has been such a disaster or catastrophic failure. Contractor must inform County of the scale and quantity of County Data loss, Contractor's intended actions to recover County Data from backups and mitigate any deleterious effect of County Data and services loss, and corrective action Contractor will take to prevent future loss. Contractor must conduct an investigation of the disaster or catastrophic failure and must share the report of the investigation with County. Contractor must cooperate fully with

County, its agents and law enforcement related to this failure. During the performance of the Contract, Contractor is responsible for any loss or damage to this material and County Data while it is in Contractor's possession, and any such loss or damage must be restored at the expense of Contractor.

11. **Third Party Software/Product/Services**
(1) Definition. "Third Party software/product/services" shall mean software, product and/or services (e.g., a cloud service), which are subject to a separate, third party license agreement.
(2) Contract Terms. Contractor may offer or enable access to Third Party software, product, and/or services that may require acceptance by County of third party license or support terms. Contractor must provide County with the applicable license or support terms for use of Third Party software/products/services prior to the execution of this this Contract or prior to Contractor's or County's use of Third Party software/product/services in the event such Contractor's services as described in Attachment A uses Third Party software/product/services at a later time then than the time this Contract is executed. Failure to provide third party license or support terms as stated herein shall constitute grounds for termination of this Contract. County reserves the right to either accept or reject the use of Third Party software/product/services.
(3) Exclusion. Professional services performed by subcontractors hired by Contractor to assist in providing the services described in Attachment A are not considered Third Party software/product/services for purposes of this Contract. Contractor will remain responsible for the fulfilment of its obligations under this Contract and for payment and performance of any such subcontractor's services.
(4) Disclaimer. Contractor is not a party to any third party contracts (e.g., pass through license or support terms) and is not responsible for and has no liability to County for its use of Third Party software/product/services. This disclaimer however does not apply to Contractor's obligation as stated under [insert here the reference to the Intellectual Property Indemnification paragraph].

12. **Default – Reprocurement Costs:** In case of Contract breach by Contractor, resulting in termination by County, County may procure the goods and/or services from other sources. If the cost for those goods and/or services is higher than this Contract, Contractor will be responsible for paying County the difference between the Contract cost and the price paid, and County may deduct this cost from any unpaid balance due Contractor. The price paid by 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 Contractor's Project Manager and County's Project Manager, such matter shall be brought to the attention of County Deputy Purchasing Agent by way of the following process:

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

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

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

Any final decision of County shall be expressly identified as such, shall be in writing, and shall be signed by County Deputy Purchasing Agent or his designee. If County does not render a decision within ninety (90) calendar days after receipt of Contractor's demand, it shall be deemed a final decision adverse to Contractor's contentions. Nothing in this paragraph shall be construed as affecting County's right to terminate the Contract for cause or for convenience as provided in Paragraph K, Termination.

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

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

1. Contractor has made false certification, or

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

15. **Emergency/Declared Disaster Requirements:** In the event of an emergency or if Orange County is declared a disaster area by County, state or federal government, this Contract may be subjected to unusual usage. Contractor shall service County during such an emergency or declared disaster under the same terms and conditions that apply during non-emergency/disaster conditions. The pricing in this Contract shall apply to serving County's needs regardless of the circumstances. If Contractor is unable to supply the goods/services under the terms of the Contract, then Contractor shall provide proof of such disruption and a copy of the invoice for the goods/services from 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 Contractor shall show both the emergency purchase order number and the Contract number.

16. **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, prior to submission to County. Contractor agrees that County review is discretionary and Contractor shall not assume that County will discover errors and/or omissions. If 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 County or others discover errors or omissions in the reports, files or other written documents submitted by 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 County and Contractor, and the reports, files or documents will be returned to Contractor for correction.

17. **Equal Employment Opportunity:** 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. 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, 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. 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. 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.

18. **News/Information Release:** Contractor shall not issue any news releases or make any contact with the media in connection with either the award of this Contract or any subsequent amendment of or effort under this Contract. Contractor must first obtain review and written consent of said news releases from County through County's DPA.

19. **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:	Altarum Institute
	Attention:	David Banks
	Address:	2500 Wilson Blvd., Suite 400 Arlington, VA 22201
	Telephone:	202-776-5111
	E-mail:	David.Banks@altarum.org, with copy to legal@altarum.org
For County:	Name:	County of Orange HCA/Procurement and Contract Services
	Attention:	Roland Tabangin, DPA
	Address:	200 W. Santa Ana Blvd Suite 650 Santa Ana, CA 92701
	Telephone:	(714) 834-XXXX
	E-mail:	rtabangin@ochca.com
CC:	Name:	County of Orange HCA Epidemiology Reception
	Attention:	Josh Jacobs
	Address:	1719 W 17th St., Ste 119 Santa Ana CA 92706
	Telephone:	714-834-8139
	E-mail:	jjacobs@ochca.com

20. **Ownership of Documents:** County has permanent ownership of all directly connected and derivative materials produced under this Contract by Contractor. All documents, reports and other incidental or derivative work or materials furnished hereunder shall become and remain the sole property of County and may be used by County as it may require without additional cost to County. None of the documents, reports and other incidental or derivative work or furnished materials shall be used by Contractor without the express prior written consent of County.

21. **Precedence:** The Contract documents consist of this Contract and its Attachments. 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, then the Attachments.

22. **Promotional/Advertisement:** County owns all rights to the name, trademarks, logos and symbols of County. The use and/or reproduction of County's name, trademark, logo and/or symbol for any purpose, including commercial advertisement, promotional purposes, announcements, displays or press releases, without County's express prior written consent is expressly prohibited. No use or reproduction may state or imply that County endorses Contractor's products or services.

23. **Publication:** No copies of sketches, schedules, written documents, computer-based data, photographs, maps or graphs, including graphic artwork, resulting from performance or prepared in connection with this Contract, are to be released by Contractor and/or anyone acting under the supervision of Contractor to any person, partnership, company, corporation, or agency, without County's express prior written consent, except as necessary for the performance of the services of this Contract. All press contacts, including graphic display information to be published in newspapers, magazines, etc., are to be administered by County or only after County approval.

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

25. **Subcontracting:** No performance of this Contract or any portion thereof may be subcontracted by Contractor without the express written consent of County. Any attempt by Contractor to subcontract any performance of this Contract without the express written consent of County shall be invalid and shall constitute a breach of this Contract.

    In the event that Contractor is authorized by County to subcontract, this Contract shall take precedence over the terms of the Contract between Contractor and subcontractor and the subcontract shall incorporate by reference the terms of this Contract. County shall look to Contractor for performance and indemnification and not deal directly with any subcontractor. All work performed by a subcontractor must meet the approval of the County of Orange.

26. **Termination – Orderly:** If County terminates this Contract, Contractor may submit to County a termination claim, if applicable, after receipt of the termination notice.

Contractor's claim must be submitted promptly, but in no event later than sixty (60) calendar days from the effective date of the termination, unless one or more extensions in writing are granted by County upon written request of Contractor. County agrees to pay Contractor for all services satisfactorily performed prior to the effective date of the termination that meet the requirements of the Contract according to the compensation provisions contained in this Contract; provided, however, that such compensation combined with previously paid compensation shall not exceed the total compensation set forth in this Contract. Upon termination or other expiration of this Contract, each party must promptly return to the other party all papers, materials, and other properties of the other held by each for purposes of execution and performance of this Contract and transfer all assets, tangible and intangible, as may be necessary for the orderly, non-disruptive business continuation of each party. Contractor shall return all County Data to County in the file format specified by County within thirty (30) calendar days.

In addition, Contractor at its own expense shall erase, destroy, and render unreadable all data in its entirety remaining in Contractor's (including any subcontractor's) possession and any system Contractor directly or indirectly uses or controls, and any copies thereof, but only after the County Data has been returned to County. County Data must be rendered in a manner that prevents its physical reconstruction through the use of commonly available file restoration utilities. Certification in writing that these actions have been completed must be provided within thirty (30) calendar days of termination or expiration of this Contract or within seven (7) calendar days of a request of County, whichever shall come first. To the extent that any applicable law prevents Contractor from destroying or erasing County Data as set forth herein, Contractor shall retain, in its then current state, all such County Data then within its right of control or possession in accordance with the confidentiality, security and other requirements of this Contract, and perform its obligations under this paragraph as soon as such law no longer prevents it from doing so.

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

28. **Usage Reports:** Contractor shall submit usage reports on an annual basis to the assigned DPA. The usage report shall be in a format specified by the user department and shall be submitted ninety (90) calendar days prior to the expiration date of the contract term, or any subsequent renewal term, if applicable.

29. **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).

30. **Debarment:** Contractor certifies that neither Contractor nor its employee(s) are presently debarred, proposed for debarment, declared ineligible or voluntarily excluded from participation in the transaction by any state or federal department or agency. County has the right to terminate this Contract for cause pursuant to Paragraph K, Termination, if Contractor is or becomes the subject of any debarment or pending debarment, declared ineligible or voluntary exclusion from participation by any state or federal department or agency.

31. **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, 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.

32. **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.

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

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

35. **Non-Exclusivity:** Nothing herein shall prevent County from providing for itself or obtaining from any third party, at any time during the term or thereafter, the services, or any type of products or services in any way analogous, similar, or comparable to the services, as applicable, or any other products or services.

36. **Right to Access and Use Services:** Contractor grants County a non-transferable and non-exclusive right to use and access Contractor's system, including all functionalities and services provided, furnished or accessible under this Contract, described in Attachment A, Scope of Work ("System"). This includes the right of County to, and access to, all System maintenance and warranty updates, upgrades, new releases, patches, corrections, modifications, enhancements, fixes and support without Contractor requiring a separate maintenance or support agreement. County may use the System with any

computer, computer system, server or desktop workstation owned or utilized by County or other authorized users.

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

Policies and Procedures

Contractor and Contractor's subcontractors, personnel, and all other agents and representatives of Contractor, shall at all times comply with and abide by all policies and procedures of County as they now exist or may hereafter be created, changed, modified, amended, supplemented or replaced by County from time to time, in its sole discretion, that are provided or available to Contractor in connection with Contractor's performance under this Contract. Contractor shall cooperate with County in ensuring Contractor's compliance with County policies and procedures described in this Contract and as adopted by County from time-to-time, and any material violations or disregard of such policies or procedures shall, in addition to all other available rights and remedies of County, be cause for termination of this Contract.

Security and Policies

All performance under this Contract shall be in accordance with County's security requirements, policies, and procedures as set forth in this Paragraph. Contractor shall at all times use industry best practices and methods with regard to the prevention, detection, and elimination, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County Resources (which is defined as all applicable County systems, software, assets, hardware, equipment, and other resources owned by or leased or licensed to County or that are provided to County by third party service providers) and County Data accessed in the performance of Services in this Contract. Contractor also must comply with Attachment D, Business Associate Contract.

Information Access

Contractor must at all times use appropriate safeguard and security measures to ensure the confidentiality and security of all County Data and County Resources. All County Data and County Resources used and/or accessed by Contractor: (a) must be used and accessed by Contractor solely and exclusively in connection with, and in furtherance of, the performance of Contractor's obligations under this Contract; (b) must not be used or accessed except as expressly permitted in this Contract and must not be commercially exploited in any manner whatsoever by Contractor or Contractor's personnel and subcontractors; and (c) must not be shared with Contractor's parent company or other affiliate without County's express prior written consent.

County may require Contractor to issue any necessary information-access mechanisms, including access IDs and passwords, to Contractor personnel and subcontractors, only with such level of access as is required for the individual to perform the individual's assigned tasks and functions under this Contract. The issued mechanisms may not be shared and may only be used by the individual to whom the information-access mechanism is issued. In addition, the issued mechanisms must be promptly cancelled when the individual is terminated, transferred or on a leave of absence. Each calendar year of the Contract and any time upon request by County, Contractor must provide County with an accurate, up-to-date list of those Contractor personnel and subcontractors

with access to County Data and/or County Resources and the respective security level or clearance assigned to each such individual.

Contractor, including Contractor personnel and subcontractors, must fully comply with all of County's policies and procedures regarding data access and security, including those prohibiting or restricting remote access to County Data and County Resources. County may require all Contractor personnel and subcontractors performing Services under this Contract to execute a confidentiality and non-disclosure Contract Contract concerning County Data and County Resources in the form provided by County. Contractor's failure to comply with the provisions of this Paragraph is a breach of this Contract and entitles County to deny or restrict the rights of such non-complying Contractor personnel to access and use the County Resources and County Data, as County in its sole discretion deems appropriate.

Data Security Requirements

Without limiting Contractor's obligation of confidentiality as further described in this Contract, Contractor must establish, maintain, and enforce a data privacy program and an information security program, including safety, physical, and technical security policies and procedures, that comply with the requirements set forth in this Contract and, to the extent such programs are consistent with and not less protective than the requirements set forth in this Contract, are at least equal to applicable best industry practices and standards. These programs must provide physical and technical safeguards against accidental, unlawful, or unauthorized access to or use, destruction, loss, alteration, disclosure, transfer, commingling, or processing of County Data. Contractor must take all necessary measures to secure and defend all locations, equipment, systems, and other materials and facilities employed in connection with the Services against "hackers" and others who may seek, without authorization, to disrupt, damage, modify, access or otherwise use Contractor Resources (which is defined as all Services, software, assets, hardware, equipment, and other resources and materials provided by Contractor to County, otherwise utilized by Contractor, or approved by Contractor for utilization by County, in connection with this Contract) or the information found therein; and prevent County Data from being commingled with or contaminated by the data of other customers or their users. Contractor also must continuously monitor Contractor Resources for potential areas where security could be breached. Contractor must review the data privacy and information security programs regularly, but no less than annually, and update and maintain them to comply with applicable laws, regulations, technology changes, and best practices.

Without limiting County's audit rights in this Contract, County has the right to review Contractor's data privacy program and information security program prior to commencement of Services and from time to time during the term of this Contract. Contractor must allow County reasonable access to Contractor's security logs, latency statistics, and other related security data that affect this Contract and County Data, at no cost to County. In addition, during the term of this Contract from time to time without notice, County, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program. Contractor must implement any required safeguards as identified by County or by any audit of Contractor's data privacy and information security program. County reserves the right, at its sole discretion, to immediately terminate this Contract or a part thereof for cause pursuant to

Paragraph K, Termination, if County reasonably determines Contractor fails or has failed to meet its obligations under this Paragraph.

Enhanced Security Measures

County may, in its discretion, designate certain areas, facilities, or County Resources as requiring an enhanced level of security and access control above that expressly required in this Contract. County will notify Contractor in writing reasonably in advance of any such designation becoming effective. The notice will set forth in reasonable detail the enhanced security or access-control procedures, measures, or requirements that Contractor must implement and enforce as well as the date on which such procedures and measures will take effect. If commercially reasonable, Contractor, including Contractor's personnel and subcontractors, must fully comply with and abide by all such enhanced security and access measures and procedures as of such date. If not commercially reasonable to fully comply as of such date, Contractor, including Contractor's personnel and subcontractors, must fully comply with and abide by all such enhanced security and access measures and procedures within a commercially reasonable time. County will be responsible for any additional cost required by the changes.

General Security Standards

Contractor is solely responsible for the Contractor Resources used by or for Contractor to access County Resources, County Data or otherwise in connection with the Services and must prevent unauthorized access to County Resources or County Data through the Contractor Resources. At all times during the term, Contractor must maintain a level of security with regard to the Contractor Resources, that in all events is at least as secure as the levels of security that are common and prevalent in the industry and in accordance with industry best practices. Contractor must maintain all appropriate administrative, physical, technical, and procedural safeguards and controls to secure County Data from data breach, protect County Data and the Services from loss, corruption, unauthorized disclosure, and from hacks, and the introduction of viruses, Disabling Devices, malware, and other forms of malicious and inadvertent acts that can disrupt County's access and use of County Data and the Services. Such measures must include at a minimum: (a) access controls on information systems, including controls to authenticate and permit access to County Data only to authorized individuals and controls to prevent Contractor employees from providing County Data to unauthorized individuals who may seek to obtain this information; (b) industry-standard firewall protection; (c) encryption of electronic County Data while in transit from Contractor networks to external networks; (d) measures to store in a secure fashion all County Data which must include but not be limited to, encryption at rest and multiple levels of authentication; (e) dual control procedures, segregation of duties, and pre-employment criminal background checks from employees with responsibilities for or access to County Data; (f) measures to ensure that County Data is not altered or corrupted without the prior written consent of County; (g) measures to protect against destruction, loss or damage of County Data due to potential environmental hazards, such as fire and water damage; (h) staff training to implement the information security measures; and (i) monitoring of the security of any portions of Contractor Resources that are used in the provision of the Services against intrusion on a twenty-four hour a day basis.

Security Failures

County has the right to immediately terminate this Contract with cause pursuant to Paragraph K, Termination, and the right to receive Contractor's payment of any pre-paid fees prorated to the date of termination if County in its sole discretion determines there is a Security Failure. A "Security Failure" means Contractor or its subcontractors, or the employees or agents of the foregoing, do not meet the security requirements of this Contract, including any backup, disaster recovery, or other policies, practices, or procedures related to security of County Data and County Resources. The remedy provided in this Paragraph is not exclusive and is in addition to any other rights and remedies provided by law or under this Contract.

Security Breach Notification

In the event Contractor becomes aware of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access, that compromises or is suspected to compromise the security, confidentiality, or integrity of County Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the security, confidentiality, or integrity of County Data, Contractor shall, at its own expense, (1) immediately notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence and perform a root cause analysis thereon, (2) investigate such occurrence, (3) provide a remediation plan, acceptable to County, to address the occurrence and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event, and (5) cooperate with County and any law enforcement or regulatory officials investigating such occurrence, including but not limited to making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by County and/or any law enforcement or regulatory officials, and (6) perform or take any other actions required to comply with applicable law as a result of the occurrence (at the direction of County). County shall make the final decision on notifying County persons, entities, employees, service providers, and/or the general public of such occurrence, and the implementation of the remediation plan. If notification to particular persons is required under any law or pursuant to any of County's privacy or security policies, then notifications to all persons and entities who are affected by the same event shall be considered legally required. Contractor shall reimburse County for all notification related costs incurred by County arising out of or in connection with any such occurrence due to Contractor's acts, errors or omissions, negligence, and/or misconduct resulting in a requirement for legally required notifications.

In the case of personally identifiable information, Contractor shall provide third-party credit and identity monitoring services to each of the affected individuals for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twelve (12) months following the date of notification to such individuals.

In addition to indemnity obligations set forth elsewhere in this Contract, Contractor shall indemnify, defend and hold County and County Indemnitees harmless from and against any and all claims, including reasonable attorneys fees, costs, and expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from County in connection with the occurrence**.**

Ed Althof, Assistant Chief Information Officer 1055 N. Main St, 6th Floor Santa Ana, CA 92701 Office: (714) 834-3069 E-mail: ed.althof@ocit.ocgov.com	Linda Le, CHPC, CHC, CHP County Privacy Officer 1055 N. Main St, 6th Floor Santa Ana, CA 92701 Office: (714) 834-4082 Email: linda.le@ocit.ocgov.com securityadmin@ocit.ocgov.com

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

Contractor shall maintain complete and accurate records relating to its SOC Type II or equivalent's data protection practices and the security of any of County Data, including any backup, disaster recovery, or other policies, practices or procedures. Further, Contractor shall inform County of any security audit or assessment performed on Contractor's operations, information security program, or disaster recovery plan that includes County Data, within sixty (60) calendar days of such audit or assessment. Contractor will provide a copy of the audit report to County within thirty (30) days after Contractor's receipt of request for such report. If Contractor does not perform a SOC Type II or equivalent audit at least once per calendar year, County may perform or have performed by an independent security expert its own such security audits, which may include penetration and security tests of Contractor Systems and operating environments. All such testing shall ensure all pertinent County security standards as well as any HCA/Environmental Health requirements (e.g., such as federal tax requirements or HIPAA) are in place. Contractor shall reasonably cooperate with all County security reviews and testing, including but not limited to, penetration testing. Contractor shall implement any required safeguards as identified by County or by any audit of Contractor's data privacy and information security program. In addition, Contractor will provide to County upon request the most recent third-party SOC 2 Type II report. County may also

have the right to review Plans of Actions and Milestones (POA&M) for any outstanding items identified by the SOC 2 Type II report requiring remediation as it pertains to the confidentiality, integrity, and availability of County Data. County reserves the right, at its sole discretion, to immediately terminate this Contract or a part thereof without limitation and without liability if County reasonably determines Contractor fails or has failed to meet its obligations under this paragraph.

38. **Extraction of County Data:** During the term of this Contract, County is able to extract County Data from Contractor's system without cost at any time. For up to thirty (30) calendar days after termination or expiration of this Contract, cessation of business by Contractor, or any other event preventing Contractor from continuing to perform under this Contract, Contractor must provide County an extract of County Data in the format specified by County within five (5) business days of County's request.

    The extraction of County Data by Contractor is without cost and not subject to any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Contractor). Contractor cannot withhold County Data or refuse for any reason to promptly return to County all County Data (including copies thereof) requested by County, even if County is then or is alleged to be in breach of the Contract. As part of Contractor's obligation to provide County Data, Contractor will also provide County any data maps, documentation, software, or other materials necessary for County to use, translate, interpret, extract and convert County Data.

39. **Data Location:** Except where Contractor obtains County's express prior written consent, the physical location of Contractor's data center where County Data is stored must be within the United States. Any time County Data is relocated within the United States, Contractor must securely dispose of such copies from the former data location and certify in writing to County that such County Data has been disposed of securely. Contractor must comply with all reasonable directions provided by County with respect to the disposal of County Data. Further, should it become necessary in the course of normal operations for Contractor to copy or move County Data to another storage destination on its online system and delete County Data found in the original location, Contractor must preserve and maintain the content and integrity of County Data.

40. **Trans-Border Data Flow:** Contractor must not transfer any County Data across a country border. Furthermore, Contractor must perform all services required under this Contract within the United States and must not access County Data from outside the United States.

41. **Documentation:** Contractor must provide to County, at no charge, all documentation, and updated versions thereof, including but not limited to manuals and other printed materials, necessary or useful to County in its use or access of Contractor's system. Contractor agrees that County may reproduce such documentation for its own use. County agrees to include Contractor's copyright notice on any such documentation reproduced in accordance with any copyright instructions provided by Contractor.

42. **No Third-Party Beneficiaries:** This Contract is an Contract Contract by and between the Parties and does not: (a) confer any rights upon any of the employees, agents, or contractors, of either Party or upon any other person or entity not a party hereto; or (b) preclude any actions or claims against, or rights of recovery from, any person or entity not a party hereto.

43. **Discovery:** Contractor shall promptly notify County upon receipt of any requests which in any way might reasonably require access to County Data to which Contractor or any third party hosting service of Contractor may have access or to County's use of Contractor's services. Contractor shall notify County by the fastest means available and also in writing, with additional notification provided to the County's Project Manager or designee, unless prohibited by law from providing such notification. Contractor shall provide such notification within forty-eight (48) hours after Contractor receives the request. Contractor shall not respond to subpoenas, service of process, Public Records Act requests, and other legal requests directed at Contractor regarding this Contract without first notifying County, unless prohibited by law from providing such notification. Contractor must provide its intended responses to County with adequate time for County to review, revise, and, if necessary, seek a protective order in a court of competent jurisdiction. Contractor shall not respond to legal requests directed at County unless authorized in writing to do so by County.

(SIGNATURE PAGE FOLLOWS)

Signature Page

IN WITNESS WHEREOF, the Parties hereto have executed this Contract No. MA-042-23010683 on the date set forth opposite their signatures. If Contractor is a corporation, Contractor shall provide two signatures as follows: 1) the first signature must be either the Chairman of the Board, the President, or any Vice President; 2) the second signature must be either the Secretary, an Assistant Secretary, the Chief Financial Officer, or any Assistant Treasurer. In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution or by-laws demonstrating the legal authority of the signature to bind the company.

Contractor: Altarum Institute

Michael Monson	President & CEO
Print Name	Title
DocuSigned by: Michael Monson D6C9FA0F7909432...	7/20/2023
Signature	Date
Denise Sturm	Chief Financial Officer
Print Name	Title
DocuSigned by: Denise Sturm 0D094539E4604A6...	7/24/2023
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 McLean (for Massoud Shamel)	Deputy County Counsel
Print Name	Title
DocuSigned by: Brittany McLean (for Massoud Shamel) 9713A4061D4343D...	
Signature	

Attachment A – Scope of Work

A. Background

Public Health Services (PHS) is the service area of Orange County Health Care Agency (OCHCA) that monitors and investigates the occurrence of disease, injury, and related factors in the community and in collaboration with community partners to develop and implement preventive strategies to maintain and improve the health of the public. Divisions in Public Health Services include California Children's Services, Clinical Services, Communicable Disease Control, Community and Nursing Services, Health Promotion and Community Planning, and Public Health Laboratory. Programs in each division work with other Health Care Agency service areas and community partners to provide vital services to the residents of Orange County.

MDROs are infectious pathogens that are resistant to multiple antibiotic or antifungal agents. Spread of these types of pathogens primarily occur in healthcare settings and are a worldwide public health concern. In 2022, 10,791 individual MDRO cases were reported to Orange County Public Health Services from Orange County acute care hospitals (ACH), long term acute care hospitals (LTACH), and skilled nursing facilities (SNF).

A critical component of mitigating the spread of MDROs in healthcare facilities is to ensure timely and effective reporting/notification of patient MDRO status during the patient interfacility transfer process. MDRO data exchanges have been established in multiple jurisdictions around the country to some extent to provide consistent electronic communication between healthcare facilities and from those facilities to public health. OCHCA has received requests from infection preventionists at multiple Orange County hospitals to develop an MDRO data exchange to support the interfacility patient transfer process which will minimize inadvertent MDRO exposures through a consistent and timely communication process with public health, and protect patients from exposure to these potentially deadly pathogens.

Objective

OCHCA PHS's objective is to establish a Multi-Drug Resistant Organism (MDRO) Data Exchangeplatform, allowing for County acute care hospitals (ACH), long term acute care hospitals (LTACH), skilled nursing facilities (SNF), and local Public Health to register/enter, store, and readily access basic demographic and laboratory data for persons who test positive for MDROs including Candida auris (C. auris), Methicillin-resistant Staphylococcus (MRSA), Extended-spectrum beta-lactamases (ESBL), and Carbapenem-resistant Enterobacter ales (CRE). Implementation of the registry will result in a more effective disease control approach with the goal of minimizing (and potentially eliminating) inadvertent exposures and transmissions of MDROs and safeguarding patient health.

The system will allow participating facilities to enter patients colonized or infected with a MDRO through a secure Web Portal and fully automate the notification process to notify OC HCA PHS, Communicable Disease Control Division, and the

admitting facility. This will increase efficiency during the patient intake processes at facilities and support timelier PHS investigation efforts to quickly identify patient MDRO status to reduce inadvertent MDRO exposures in the transfer facility. The system will also allow HCA and participating facilities to produce reports to provide timely updates of specified information at both the facility and public health levels, as well as to illustrate trends and inform decision making.

B. System Components

The system shall support all functional activities that support Orange County Public Health Services requirements for the exchange and reporting of information for patients with known MDROs. This system shall meet at least all the functional requirements listed below:

1. Customized secure cloud-based platform to register patients colonized or infected with an MDRO between participating facilities and the Orange County Health Care Agency Public Health Services and have automated responses notifying OCHCA and the admitting facility to increase efficiencies and timely availability of information in the patient intake processes and investigations to identify patient status and MRDO history to reduce inadvertent MDRO exposures..
    a. Web portal that allows external facilities (ACH, LTACH, and SNF) to submit patient registry data to the data exchange for reporting. The features of this module shall include:
        i. The data exchange shall have the ability to access, upload, store, report and share relevant information for patients with known MDROs including C auris, MRSA, ESBL, VRE and CRE, as well as any new emerging MDROs. The exchange shall develop and maintain a centralized master patient index (MPI) of patients colonized or infected with an MDRO and integrate with existing MPI schemas present within the county and the partner organizations. This includes support for various internal business workflows, reports and analytics, security, online web portal for all authorized users and all access methods.
        ii. Any participating health care facility staff shall be able to manually enter relevant patient demographic and other relevant data into the exchange.
        iii. The data exchange shall have the ability for participating health care facility staff to update their own existing registry records as required.
        iv. The data exchange shall support the creation and maintenance of user-defined data fields in all common data formats to allow full support for all required data fields from the participating facilities' existing registry records, and have this be available from all aspects including storage, reporting, sharing, printing, and forms.
        v. Participating facilities shall have the ability of automatically checking their daily patient admission lists against the MPI in the exchange. If a newly admitted patient is identified to

have an MDRO by this process, an automated message (such as an email) shall be automatically forwarded to designated staff at the admitting facility for notification.

vi. The data exchange shall allow participating facilities the option of entering patient MDRO results through electronic reporting.

vii. The data exchange shall allow patient information to be accessible to designated staff in each participating facility, with information for all patients easily reviewable by search.

viii. The data exchange shall allow accurate patient matching and facility identification using the MPI logic.

ix. Patient information entered into the system shall be available to other facilities for review in a timely fashion in real time or near real time basis.

x. The data exchange architecture shall comply with all applicable current and emerging state and federal data exchange and health data privacy and security requirements.

xi. The data exchange shall allow the ability to inform participating facilities based on their preferred delivery method when a newly admitted patient is identified to have a MDRO by this process through a proactive versatile notification system.

xii. The data exchange shall allow the ability to handle large dynamic sets of entries at any given time. The system shall support appropriate scaling to enable optimal performance for handling demand and utilization surges, especially during future outbreaks, epidemics, and pandemics.

2. The system shall meet the following Data Exchange Storage and Management Functionality:
    a. The data exchange shall serve as a repository for storing and maintaining records.
    b. All data gathered through this Contract shall constitute County Data, as defined in Paragraph 10 of the main Contract (titled, “County Data and Ownership”) and shall be subject to the provisions of Paragraph 10. While maintaining the system and data through the life of the Contract, the Contractor shall work with OCHCA to develop acceptable standards, policies and procedures for the overall management, retention, reporting, monitoring and auditing of all data.
3. The system shall provide ongoing support of the data exchange to assure appropriate functionality and accuracy. The system shall be structured to assure ongoing assessment of the following:
    a. Functionality and accuracy
        i. Assess the initial build for core functionality and accuracy in exchanging patient infection or colonization status from an identifying facility (i.e., facility in which patient colonization status was detected) to an admitting facility, with accurate delivery of minimum data elements.
        ii. Determine proportion of infected or colonized patient transfer and admission events are accurately reported

across each of the minimum data elements.

b. Reduce unnecessary burden
    i. Assess the time required to perform any manual processes of reporting into the exchange or accessing information from the exchange.
c. Utilization of the exchange
    i. Review the proportion of all MDRO-infected or -colonized patient transfers or admissions, as determined by health record audit, that are reported into the exchange, along with the proportion of exchange-reported events accessed by receiving/admitting facilities.
d. Timeliness
    i. Determine the time after admission or transfer receipt by which MDRO infection or colonization status becomes accessible to receiving facility.
    ii. Determine the time after admission or transfer receipt by which an order for appropriate Transmission-Based Precautions is placed at a receiving facility.
e. Health Information Exchange (HIE) and Electronic Medical Records (EMR) integration.
    i. The system shall have HIE interoperability with other systems, as required.
    ii. The system shall have EMR interoperability with other systems, as required.

Data Elements for Patient, Facility, and MDRO Identification

1. Name
2. Date of birth (DOB)
3. Sex
4. Address
5. Phone number
6. Unique patient ID
7. Event type (patient movement (admission, discharge, or transfer) and/or new MDRO identification)
8. Facility name (facility with the current encounter) of triggering event
9. Facility address (facility with the current encounter) of triggering event
10. MDRO (e.g., name of organism and type/category of resistance)
11. Specimen collection date corresponding to first positive laboratory result
12. Specimen collection date corresponding to most recent positive laboratory result

Other Data Elements

1. Patient information
    a. Medication allergies
    b. Race
    c. Ethnicity
    d. Preferred language
    e. Gender
    f. Patient travel history

i. Last date of travel outside of the United States (including country(ies) visited)
ii. Last date the patient received healthcare outside the United States (including which country(ies))

g. Past infectious diseases
   i. Past infectious disease diagnosis
   ii. Past infectious disease diagnosis date
h. Current Diagnostic information
   i. Diagnosed infectious condition(s)
   ii. Date(s) of diagnosis(es)
i. Healthcare Acquired Infection (HAI) information
   i. Does the patient have a healthcare-associated infection? (Y/N)
   ii. Is the patient on Transmission-Based Precautions?
   iii. If yes, what type of precautions?
j. Pathogen information
   i. Specimen source
k. Phenotype
   i. Genus and species name
   ii. Current pathogenic carrier state (e.g., infected versus colonized)
   iii. Mechanism of resistance
l. Diagnosing laboratory information
   i. Laboratory reporting the MDRO
   ii. Date(s) of specimen collection
m. Treatment information
   i. Antibiotic(s) indication
   ii. Antibiotic(s) start date
   iii. Antibiotic(s) dosage
   iv. Antibiotic(s) route of administration
   v. Antibiotic(s) intended duration
   vi. Facility information
   vii. For all relevant facilities (e.g., admitting, transferring, discharging, ambulatory): Name, address, unit number, phone number, unique facility ID, and point(s) of contact
n. Procedures
   i. Procedures
   ii. Current or recent invasive medical device
o. Location of invasive medical device

C. Reports

This solution shall allow OCHCA and participating facilities to produce reports to provide timely updates of specified information at the facility and public health levels. The system shall generate reports using a reporting wizard and shall have the ability to:

1. Create canned and ad-hoc reports.
2. Ability to customize up to five (5) OCHCA selected reports using built-in reporting tool
3. Design and run reports using a report wizard.
4. Export data to common data formats.

5. Publish reports as an automated data feed to external websites through API.
6. Restrict report creation by access roles.
7.
8. Ability to support use of data by County approved data visualization tools if needed.
9. Support compliance related reports such as access monitoring and auditing.

D. Technology Requirements

1. The system shall be a Software as a Service model in the cloud accessible to suit HCA Service Areas and shall meet HCA IT Security requirements. This should follow a high-performance sustainable IT infrastructure and include a multi-tenancy model for optimal availability.

2. Ensure that the application will have a continuous cycle of review and updates by the vendor, by following a mutually acceptable change management policy.

3. The SaaS platform shall follow an industry standard framework to allow for seamless and optimal integration with other systems.

4. The SaaS framework management and governance shall include processes and policies that encompass physical, network, application, and data-level security, as well as full back-up and disaster recovery strategies.

5. The overall architecture shall support demand-based elasticity and scalability to consistently meet established service level expectations in terms of performance and availability.

6. The system shall have a high degree of usability and user-friendliness with the following qualities:

    a. A clean user interface that’s visually appealing.

    b. Intuitive operation that’s familiar to the user, including straightforward navigation data-entry, reviewing data, and running reports.

7. The system shall have the ability to support all current web browser types.

8. The system will have the ability to integrate with Orange County Identity Management Solution (Microsoft Azure Active Directory) for authentication of Orange County users and support the creation of local accounts within the data exchange platform for use by participating facilities.

9. The system shall provide safeguards for referential integrity of all data.

10. All data transmissions and data at rest must be encrypted using a current FIPS compliant algorithm which is 256-bit or higher.

11. The system shall be implemented using Multi-Factor Authentication (MFA) for all local accounts managed within the data exchange system MFA for Orange County users will be managed via Microsoft Azure Active Directory.

12. The system shall be scalable to accommodate additional users and modules as needed.
13. The system shall be web-based and have a 99.9% up time.
14. The system shall be accessible 24 hours a day, 7 days a week.

E. Mobility Requirements

1. The system shall be device agnostic, i.e., application performance shall be identical whether the end user is connecting from a desktop or a tablet or any mobile device.
2. Menus and forms shall scale to display appropriately on any device, regardless of screen resolution, aspect ratio, or orientation.
3. The system shall be designed for optimal performance over slower or unreliable connections.
4. The system shall be designed with the primary expected input methods using drop-down lists, and context-specific fields.
5. If required for functional use, the application shall support native functions of the client device, including but not limited to on-screen keyboards, voice dictation, predictive text and suggested words, front and rear cameras, and GPS virtualization technology, whenever possible, for all new systems.

F. 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 Agile methodology.

2. Contractor and HCA shall be responsible for establishing a Project Organization Plan to manage and deliver the services defined in this Scope of Work. After execution of 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. Change Management – Contractor shall include a description of the change control management process that shall be used in order to manage changes either requested by the County or to mitigate any deviation from the plan.

4. Contractor shall develop project 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.

5. 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:
    i. Conditions warranting changes to the core team or requiring additional resources in meeting the milestones and/or resolving a problem/issue.
    ii. Time durations between escalating to next level of support.
    iii. A diagram depicting the various levels of response.
    iv. The names, titles, and phone numbers of Contractor staff responsible for response at the various levels of support.

G. Development, Testing & Training Environments

1. Contractor will maintain distinct development, testing and training domains. County will perform all testing and validation in the test domain. Contractor shall provide a detailed training plan to the County which shall be approved by the County project manager prior to go-live. Contractor training shall include “classroom led” in-person if required by County. Web-based instructor led training and recorded trainings shall also be available upon request by the County.

H. Support and Maintenance Procedures

1. Contractor shall be responsible for establishing support and maintenance procedures for the solution. Contractor shall provide all necessary documentation and procedures needed to support HCA’s use of the system on a 24/7 basis and all trainings, procedures, and documentations needed shall be completed prior to go-live. 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 provided to the following groups: Administrator, Super User, End User, Service Desk/Field Support, Software Support.
    i. 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.
    ii. 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.

iii. HCA IT 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.

iv. Administrator
Administrators shall be trained to support the front and back-end issues, generate reports, and manage the database if required.

v. Software Support
If applicable. 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.

I. User Acceptance Testing

1. Contractor shall develop test scripts with the approval of HCA project team needed to validate the solution as described in the requirements. 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 operational 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.

2. Integration & Regression Testing

   Successful regression testing shall be completed and signed off by the project team and the project owners for final acceptance of the product.

3. Final acceptance will occur through a coordinated and mutually acceptable process with all stakeholders and the Contractor to ensure that all deliverables meet the desired objectives and that all necessary functionality is present and error-free and is working at optimal performance.

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

Attachment B - Compensation and Invoicing

1. **Compensation**

   This is a fixed price Contract not to exceed the amount of **$3,595,000** for the Term of Contract.

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

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 C

3. **Price Increase/Decreases:** No price increases are permitted during the term of the Contract. County requires documented proof of cost increases on contracts prior to any price adjustment. A minimum of thirty (30) business 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 County. County may enforce, negotiate, or cancel escalating price contracts or take any other action it deems appropriate, as it sees fit. The net dollar amount of profit will remain firm during the period of the Contract. Adjustments increasing Contractor's profit are not allowed.

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

5. **Contractor's Expense:** Contractor is responsible for all costs related to photo copying, telephone and fax communications, travel, parking and any and all "out of pocket" expenses incurred by Contractor during the performance of work and services under this Contract, unless otherwise specified. Contractor is responsible for payment of all parking costs and expenses incurred at a County facility while performing work under this Contract, except to the extent the County facility has free parking available to the public and Contractor makes appropriate use of this free parking. However, County will not provide free parking for any service in the County Civic Center.

6. **Payment Terms –** Payment will be net thirty (30) calendar days after receipt of an invoice in a format acceptable to County and verified and approved by the /department and subject to routine processing requirements.

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

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

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

8. **Payment – Invoicing Instructions:** Contractor must provide an invoice on Contractor's letterhead for goods delivered and/or services rendered. In the case of goods, Contractor will leave an invoice with each delivery. Each invoice must have a unique number and must 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 Department
    e. Delivery/service address
    f. Master Contract Contract (MA) or Purchase Order (PO) number
    g. 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 submitted in arrears to HCAAP@ochca.com or:

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

9. **Payment (Electronic Funds Transfer)**

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

Attachment C - Cost Summary and Pricing

Year 1				Invoicing Schedule		
	Duration	Start	End	Date	Tasking Milestone	Amount
Contract Start		9/23/2023		9/23/2023	Contract Signed	
Initiation & Planning	25d	9/25/2023	10/27/2023			
Project Charter & Kick-off	10d	9/25/2023	10/6/2023			
Review & Validate Scope	5d	10/9/2023	10/13/2023			
Review & Validate Requirements	5d	10/9/2023	10/13/2023			
Project Management Plan [sub-plans/RACI/Change Mgmt]	10d	10/9/2023	10/20/2023			
Sprint 0 Planning	5d	10/16/2023	10/20/2023			
Setup Project Infrastructure Workflows and Configurations (Jira)	5d	10/9/2023	10/13/2023			
Develop Sprint Backlog/Release Schedule	5d	10/23/2023	10/27/2023			
Development & QA	240d	10/16/2023	7/30/2024			
Data Definition/Data Dictionary/Data Mapping	20d	10/16/2023	11/10/2023			
Cloud Hosting/Setup Environments	20d	10/16/2023	11/10/2023			
Architecture Design	20d	10/16/2023	11/10/2023			
Build DB/ Schema	10d	11/13/2023	11/27/2023			
Develop System Architecture	10d	11/13/2023	11/27/2023	**11/27/2023**	**Architecture & Infrastructure**	**$594,000.00**
Functional Design	15d	11/28/2023	12/15/2023			
UI/UX for MDRO Portal	11d	12/18/2023	1/3/2024			
Develop Patient/Case Loader (manual)	10d	1/4/2024	1/17/2024	**1/17/2024**	**Workflow & Forms**	**$416,000.00**
Develop Test Plan	10d	12/18/2023	1/3/2024			
Master Patient Index	15d	12/29/2023	1/18/2024			
Data Retriveal Module	15d	1/19/2024	2/8/2024			

Develop Case Alerts/Notifications	15d	2/9/2024	2/29/2024	**2/29/2024**	**User Management & Alerts**	**$298,000.00**
Secure Data Repository	10d	3/1/2024	3/14/2024			
Data Quality Assurance Mechanism	10d	3/15/2024	3/28/2024			
FHIR Gateway	10d	3/29/2024	4/11/2024	**4/11/2024**	**External Integration**	**$342,000.00**
Audit Logging	10d	4/12/2024	4/25/2024			
Requirements Gathering for Reporting Wizzard	10d	4/26/2024	5/9/2024			
Custom Query Development	10d	5/10/2024	5/23/2024			
Query module	10d	5/24/2024	6/6/2024			
API Gatway	10d	6/7/2024	6/20/2024			
Data reporting module	10d	6/21/2024	7/4/2024	**6/30/2024**	**Search & Reporting**	**$342,000.00**
Registration Procedure	10d	7/5/2024	7/18/2024			
Regression Testing	20d	7/19/2024	8/15/2024			
Final Acceptance	5d	8/16/2024	8/22/2024			
Implemetation to Production Environment	5d	8/23/2024	8/29/2024			
TA&Training	60d	5/1/2024	7/23/2024			
Identify Potential Pilots/EHR Systems	15d	5/1/2024	5/21/2024			
Execute BAA & DUA	30d	5/22/2024	7/2/2024			
Create Training Plan & Materials	30d	5/1/2024	6/11/2024			
Setup TA & Support Plan	30d	5/1/2024	6/11/2024			
Setup TA & Support Triage System	30d	5/1/2024	6/11/2024			
Provide TA & Training to Recruited Pilots	15d	7/3/2024	7/23/2024	**6/30/2024**	**Training & Support**	**$293,000.00**
Onboarding/Training Pilot Facilities	15d	7/3/2024	7/23/2024			
Deployment	100d	5/1/2024	9/17/2024			
Develop & Execute Deployment Plan	10d	5/1/2024	5/14/2024			
Final QA and Regression Testing	20d	8/16/2024	9/12/2024			
Production Go Live	3d	9/13/2024	9/17/2024	**6/30/2024**	**Testing & Deployment**	**$310,000.00**
					Base Year Total	$2,595,000.00

Year 2						
Maintenance & Operations					Total	**$500,000.00**
Training & Support						
Year 3						
Maintenance & Operations						
Training & Support					Total	**$500,000.00**

A. Administrator may, at its discretion, pay invoices in any amount, at any time during the Term of this Contract provided the Maximum Obligation for each Period is not exceeded.

B. Contractor's invoices shall be on a form approved or supplied by Administrator and provide such information as is required by Administrator.

C. Administrator may withhold or delay any payment if Contractor fails to comply with any provision of the Contract, or if sufficient progress is not being made with the program as determined by Administrator in its sole discretion.

D. County shall not reimburse Contractor for services provided beyond the expiration and/or termination of the Contract, except as may otherwise be provided under the Contract, or specifically agreed upon in a subsequent Contract.

E. Contractor and Administrator may mutually agree, in writing, to modify the Payments Paragraph of this Attachment C to the Contract.

F. Contractor Licensing Structure:

The quoted costs of this proposal include up to 500 registered users. The system can accommodate more users but there would be increased fees. User licenses, costs per connection point (of pilot sites), and costs associates with concurrent users are outlined below. These licensing fees cover the PoP for the contract.

- **User Licenses**:
  - o Includes up to 500 registered users.
  - o 10% increase in hosting and maintenance and operations costs for users over 500 and up to 1000.
  - o 12% increase in hosting and maintenance and operations costs for user >1000 and up to 1500.

- **Cost per connection of sending and receiving partners**:
  - o Includes up to 40 data provider partners/pilot sites.
  - o There is a 10% increase in hosting and maintenance and operations costs for

every 25 data providers above and beyond the base 40.

- **Costs associated with the number of users**:
  - o Includes up to 200 concurrent users.
  - o There is a 10% increase in hosting and maintenance and operations costs for every 100 concurrent users above and beyond the base 200.

Attachment D - Business Associate Contract

A. GENERAL PROVISIONS AND RECITALS

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

2. The parties agree that a business associate relationship under HIPAA, the HITECH Act, and the HIPAA regulations between the CONTRACTOR and COUNTY arises to the extent that CONTRACTOR performs, or delegates to subcontractors to perform, functions or activities on behalf of COUNTY pursuant to, and as set forth in, the Contract Contract 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 Contract Contract 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 Contract Contract upon thirty (30) days written notice in the event:

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

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

D. SECURITY RULE

1. CONTRACTOR shall comply with the requirements of 45 CFR § 164.306 and establish and maintain appropriate Administrative, Physical and Technical Safeguards in accordance with 45 CFR § 164.308, § 164.310, and § 164.312, with respect to electronic PHI

COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY. CONTRACTOR shall develop and maintain a written information privacy and security program that includes Administrative, Physical, and Technical Safeguards appropriate to the size and complexity of CONTRACTOR's operations and the nature and scope of its activities.

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

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

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

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

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

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

//

//

E. DATA SECURITY REQUIREMENTS

1. Personal Controls

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

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

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

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

2. Technical Security Controls

a. Workstation/Laptop encryption. All workstations and laptops that store PHI

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

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

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

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

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

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

g. User IDs and Password Controls. All users must be issued a unique user name for accessing PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY. Username must be promptly disabled, deleted,

or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

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

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

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

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

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

l. Access Controls. The system providing access to PHI COUNTY discloses to

CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY must use role based access controls for all user authentications, enforcing the principle of least privilege.

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

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

3. Audit Controls

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

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

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

4. Business Continuity/Disaster Recovery Control

a. Emergency Mode Operation Plan. CONTRACTOR must establish a documented plan to enable continuation of critical business processes and protection of the security of PHI COUNTY discloses to CONTRACTOR or CONTRACTOR creates, receives, maintains, or transmits on behalf of COUNTY kept in an electronic format in the event of an

emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Contract Contract 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 Contract Contract 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.

//

//

//

//

//

//

//

//

//

//

SECTION III: MODEL CONTRACT

Attachment D-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 Contract Contract 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 Contract Contract on behalf of the COUNTY.

5. "IEA" shall mean the Information Exchange Contract Contract 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 Contract Contract 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.

SECTION III: MODEL CONTRACT

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 Contract Contract between the SSA and the California Health and Human Services Agency (CHHS) and in the Contract Contract between the SSA and DHCS, known as the Information Exchange Contract Contract (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 Contract Contract 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 D to the Agreement.

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

SECTION III: MODEL CONTRACT

Attachment E - OCHCA Security Requirements and Guidelines for Vendors and Application Service Providers

County of Orange
Health Care Agency

Security Requirements and Guidelines for Application Vendors and Application Service Providers

04/2022

1 Overview

Security Requirements and Guidelines for Application Vendors and Application Service Providers

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

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

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

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

2 General Security Requirements

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

into the application for these services to continue to be active. OCHCA will provide an account with the appropriate security level to logon as a service, and an account with the appropriate administrative rights to administer the application. The account password must periodically expire, as per OCHCA policies and procedures.

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

3 Encryption

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

4 Network Application Documentation

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

5 Access Management

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

6 Password Management

- Application must support password management measures including but not limited to

password expiration, account lockout and complex passwords.

- Passwords expiration must be set to 90 days and the system must prevent the use of the previous 4 passwords.
- Accounts must be locked after five unsuccessful login attempts.
- The password must be at least 8 characters in length and a combination of letters, numbers, and special characters with at least 3 of the four following categories.
  - ♦ Uppercase letters (A through Z)
  - ♦ Lowercase letters (a through z)
  - ♦ Numeric digits (0 through 9)
  - ♦ Special Characters (! @ # $ % ^ & etc.)

7 Audit Capabilities

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

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

8 Protection from Malicious Code

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

9 Remote Support Functionality

- Provider must conform to OCHCA Vendor Remote Access Policy.

SECTION III: MODEL CONTRACT

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 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.

12 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.
- **MFA.** All cloud hosted applications that are accessible over the Internet must support

Multi Factor Authentication.

13 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 Contract Contract 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, HITRUST, ISO or SOC 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.

14 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.

15 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).

16 IT Physical Security and Access Control

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

Vendor employees are expected to:

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

17 IT Security Compliance and Training

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

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

At a minimum, the vendor is expected to:

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

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

At a minimum, the vendor is expected to:

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

18 Security Testing Recommendations

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

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

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

- The web application (i.e., the software that interacts with users at their web browsers; typically customcrafted code created by the web development team)
- The web server application (the underlying software that sends and receives information via HTTP and HTTPS, typically off-the-shelf software such as Microsoft's IIS or the open-source Apache software) □
  Any separate backend application servers that process information from the web application □

The backend database systems that house information associated with the web application.

- Infrastructure diagrams.
- Configuration host review of settings and patch versions, etc.
- Full code review.
- Identification and remediation of well-known web server, code engine, and database vulnerabilities.
- Identification and remediation of any server and application administration flaws and an exploitation attempt of same.
- Analysis of user interface, normal application behavior, and overall application architecture for potential security vulnerabilities.
- Analysis of data communications between the application and databases or other backend systems.
- Manual analyses of all input facilities for unexpected behavior such as SQL injection, arbitrary command execution, and unauthorized data access.
- Analyses of user and group account authentication and authorization controls to determine if they can be bypassed.
- Identification of information leakage across application boundaries, including the capability to enumerate other users' data and "show code" weaknesses that reveal internal application logic.
- Identification of areas where error handling is insufficient or reveals too much sensitive information.
- Identification of opportunities to write to the host file system or execute uploaded files.
- Identification of product sample files, application debugging information, developer accounts or other legacy functionality that allows inappropriate access.
- Determination as to whether or not fraudulent transactions or access can be performed.
- Attempts to view unauthorized data, especially data that should be confidential.
- Examination of client-side cached files, temporary files, and other information that can yield sensitive information or be altered and re-submitted.
- Analysis of encoded and encrypted tokens, such as cookies, for weakness or the ability to be reverse engineered.

19 Vendor Deliverables

The following items are to be provided by the vendor:

- 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

SECTION III: MODEL CONTRACT

- Security Contact Identification (24x7x365)
- Staff Related Items
  - Pre-Employment Screening Policy/Procedure
  - Background Checking Procedure
  - Ongoing Employment Status Validation Process