



CONTRACT NO. MA-042-24010451

FOR

**EMPLOYEE HEALTH SOFTWARE SOLUTION (EHSS)
SYSTEM**

BETWEEN

**COUNTY OF ORANGE
(HEALTH CARE AGENCY)**

AND

CORITY SOFTWARE, INC.

CONTRACT NO. MA-042-24010451
FOR
EMPLOYEE HEALTH SOFTWARE SOLUTION (EHSS) SYSTEM
WITH
CORITY SOFTWARE, INC.

This Contract Number MA-042-24010451 ("Contract"), is made and entered into this 1st day of January, 2024 ("Effective Date") between **Cority Software, Inc.** ("Contractor"), with a place of business at 250 Bloor Street East, 9th Floor, Box Toronto, Ontario Canada M4W1E6, 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, which are sometimes referred to individually as "Party" or collectively as "Parties".

ATTACHMENTS

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

- Attachment A – Scope of Work
- Attachment B – Compensation and Invoicing
- Attachment C – OCHCA Security Requirements and Guidelines for Contractors and Application Service Providers
- Attachment D – GS-35F-0032U

RECITALS

WHEREAS, the State of California, Department of General Services, and Cority Software, Inc. executed Agreement No. GS-35F-0032U for Hosted Software and Service Agreement, effective October 12, 2022 through October 11, 2027; and

WHEREAS, County desires to enter into a Contract with Contractor for Employee Health Software Solution System; and

WHEREAS, Contractor agrees to provide services 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 Compensation and Invoicing, attached hereto as Attachment B; and

NOW, THEREFORE, the Parties mutually agree as follows:

DEFINITIONS

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

ARTICLES

General Terms and Conditions

- A. **Governing Law and Venue:** This Contract has been negotiated and executed in the State of California and shall be governed by and construed under the laws of the State of California. In the event of any legal action to enforce or interpret this Contract, the sole and exclusive venue shall be a court of competent jurisdiction located in Orange County, California, and the Parties hereto agree to and do hereby submit to the jurisdiction of such court, notwithstanding Code of Civil Procedure Section 394. Furthermore, the Parties specifically agree to waive any and all rights to request that an action be transferred for adjudication to another county.
- B. **Entire Contract:** This Contract contains the entire contract between the Parties with respect to the matters herein, and there are no restrictions, promises, warranties or undertakings other than those set forth herein or referred to herein. Electronic acceptance of any additional terms, conditions or supplemental contracts by any County employee or agent, including but not limited to installers of software, shall not be valid or binding on County unless accepted in writing by County's Purchasing Agent or designee.
- C. **Amendments:** No alteration or variation of the terms of this Contract shall be valid unless made in writing and signed by the Parties; no oral understanding or agreement not incorporated herein shall be binding on either of the Parties; and no exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing.
- D. **Taxes:** Unless otherwise provided herein or by law, the pricing does not include California state sales or use tax. Out-of-state Contractors shall indicate California Board of Equalization permit number and sales permit number on invoices, if California sales tax is added and collectable. If no permit numbers are shown, sales tax will be deducted from payment. The Auditor-Controller will then pay use tax directly to the State of California in lieu of payment of sales tax to the Contractor.
- E. **Delivery:** Time of delivery of goods or services is of the essence in this Contract. County reserves the right to refuse any goods or services and to cancel all or any part of the goods not conforming to applicable specifications, drawings, samples or descriptions or services that do not conform to the prescribed 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.
- F. **Acceptance Payment:** See Attachment B for payment terms and schedule.

- G. **Warranty:** Contractor shall use all reasonable efforts to ensure that the software performs the functions as described in available product literature and specifications. Contractor does not make any warranties, express or implied, including the implied warranties of merchantability or fitness for any particular purpose other than for the stated purpose in the product material, to County.
- H. **Patent/Copyright Materials/Proprietary Infringement:** Contractor agrees to defend with counsel approved in writing by County, such approval not to be unreasonably withheld or delayed, and hold harmless County from and against any third party claim, suit, demand, action or proceeding arising from or relating to any breach by Contractor of such third party's intellectual property rights to the Software. In the event that any suit, action, or other proceeding is asserted or brought against County alleging a violation of any intellectual property rights of a third party based upon the use of the Software, County will promptly notify Contractor and provide it with a copy of all relevant documentation. In the event the Software is held by a court, administrative body or arbitration panel of competent jurisdiction to constitute an infringement or its use is enjoined, Contractor will, at its option, either: (i) procure for County the right to continue use of the Software; (ii) provide a modification to the Software so that its use becomes non-infringing; or (iii) replace the Software with software which is substantially similar in functionality and performance. Notwithstanding the foregoing, Contractor will have no liability to County with respect to any claim of patent, copyright or other intellectual property right infringement to the extent that the claim is based upon (i) the combination of the Software with machines, systems or devices not approved by Contractor; or (ii) the unauthorized modification of the Software; or (iii) the use of the Software not in accordance with the documentation provided in writing by Contractor to County.
- I. **Assignment:** The terms, covenants, and conditions contained herein shall apply to and bind the heirs, successors, executors, administrators and assigns of the Parties. Furthermore, neither the performance of this Contract nor any portion thereof may be assigned by Contractor without the express written consent of County. Any attempt by Contractor to assign the performance or any portion thereof of this Contract without the express written consent of County shall be invalid and shall constitute a breach of this Contract.
- J. **Non-Discrimination:** In the performance of this Contract, Contractor agrees that it will comply with the requirements of Section 1735 of the California Labor Code and not engage nor permit any subcontractors to engage in discrimination in employment of persons because of the race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, or sex of such persons. Contractor acknowledges that a violation of this provision shall subject Contractor to penalties pursuant to Section 1741 of the California Labor Code.
- K. **Termination:** In addition to any other remedies or rights it may have by law, either Party has the right to immediately terminate this Contract without penalty for cause or after 30 days' written notice without cause, unless otherwise specified. Cause shall be defined as any material breach of contract, any misrepresentation or fraud on the part of the Contractor. Exercise by County of its right to terminate the Contract shall relieve County of all further obligation. Upon termination, Contractor shall refund any prepaid fees for the then remaining portion of the Contract.

- L. **Consent to Breach Not Waiver:** No term or provision of this Contract shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the Party claimed to have waived or consented. Any consent by any party to, or waiver of, a breach by the other, whether express or implied, shall not constitute consent to, waiver of, or excuse for any other different or subsequent breach.
- M. **Independent Contractor:** Contractor shall be considered an independent contractor and neither Contractor, its employees, nor anyone working under Contractor shall be considered an agent or an employee of County. Neither Contractor, its employees nor anyone working under Contractor shall qualify for workers' compensation or other fringe benefits of any kind through County.
- N. **Performance Warranty:** Intentionally Omitted.
- O. **Insurance Provisions:** Prior to the provision of services under this Contract, Contractor agrees to purchase all required insurance at Contractor's expense, including all endorsements required herein, necessary to satisfy County that the insurance provisions of this Contract have been complied with. Contractor agrees to keep such insurance coverage, Certificates of Insurance, and endorsements on deposit with County during the entire term of this Contract. In addition, all subcontractors performing work on behalf of Contractor pursuant to this Contract shall obtain insurance subject to the same terms and conditions as set forth herein for Contractor.

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

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

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

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

Qualified Insurer

The policy or policies of insurance must be issued by an insurer with a minimum rating of A- (Secure A.M. Best's Rating) and VIII (Financial Size Category as determined by the most current edition of the **Best's Key Rating Guide/Property-Casualty/United States or ambest.com**). It is preferred, but not mandatory, that the insurer be licensed to do business in the state of California (California Admitted Carrier).

If the insurance carrier does not have an A.M. Best Rating of A-/VIII, the CEO/Office of Risk Management retains the right to approve or reject a carrier after a review of the company's performance and financial ratings.

The policy or policies of insurance maintained by Contractor shall provide the minimum limits and coverage as set forth below:

Coverage

Minimum Limits

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

Required Coverage Forms

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

The Business Auto Liability coverage shall be written on ISO form CA 00 01, CA 00 05, CA 0012, CA 00 20, or a substitute form providing coverage at least as broad.

Required Endorsements

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

- 1) An Additional Insured endorsement using ISO form CG 20 26 04 13 or a form at least as broad naming the **County of Orange its elected and appointed officials, officers, agents and employees** as Additional Insureds, or provide blanket coverage, which will state **AS REQUIRED BY WRITTEN CONTRACT**.
- 2) A primary non-contributing endorsement using ISO form CG 20 01 04 13, or a form at least as broad evidencing that the Contractor's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

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

- 1) An Additional Insured endorsement naming the **County of Orange, its elected and appointed officials, officers, agents and employees** as Additional Insureds for its vicarious liability.
- 2) A primary and non-contributing endorsement evidencing that Contractor's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

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

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

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

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

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

Insurance certificates should be forwarded to the department address listed in Paragraph 18, Notices.

If Contractor fails to provide the insurance certificates and endorsements within seven (7) calendar days of notification by CEO/Purchasing or the DPA, County may terminate the Contract without penalty.

County expressly retains the right to require Contractor to increase or decrease insurance of any of the above insurance types throughout the term of this Contract. Any increase or

decrease in insurance will be as deemed by County of Orange Risk Manager as appropriate to adequately protect County.

County shall notify Contractor in writing of changes in the insurance requirements. If Contractor does not deposit copies of acceptable Certificates of Insurance and endorsements with County incorporating such changes within thirty (30) calendar 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 specific written approval.

Q. **Change of Ownership/Name, Litigation Status, Conflicts with County Interests:** Contractor agrees that if there is a change or transfer in ownership of Contractor's business prior to completion of this Contract, and 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 shall 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 shall 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 shall 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 shall apply 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 caused by any act of God, war, civil disorder, employment strike or other cause beyond Contractor's reasonable control, provided Contractor gives

written notice of the cause of the delay to County as soon as reasonably practicable after the start of the delay and Contractor avails itself of any available remedies.

S. Confidentiality:

Contractor considers Contractor's Software and its source code, object code, design, architecture, data base schema, and related documentation and information ("Contractor Confidential Information") to be valuable intellectual property and, to the extent permitted by the California Public Records Act, County agrees (i) to protect and keep confidential the Contractor Confidential Information to the same degree that it protects its own confidential and proprietary information; (ii) not to transfer or provide the Contractor Confidential Information to third parties, on a service bureau basis or otherwise, or to disclose or make available the Contractor Confidential Information to third parties except consultants or advisers who have a "need to know" and who are bound by similar non-disclosure obligations in favor of the County; and (iii) not to reverse-engineer, decompile, translate, disassemble, duplicate, copy, reproduce, modify, transfer or distribute all or any part of the Software except as consistent with the use of the Software as set out in this Agreement.

Contractor agrees that it will protect and keep confidential to the same degree that it protects its own confidential information all information of a confidential nature received from County including, without limitation, protected health information, employee demographic information, and other information pertaining to County's employees, business processes, financials, and customers ("County Confidential Information"). The obligations with respect to Contractor Confidential Information and County Confidential Information shall continue indefinitely notwithstanding any termination of this Contract. County acknowledges and agrees that Contractor may anonymize and use County's "Anonymized Data" (defined below), combine it with data from other sources to an aggregate dataset, and use the resulting information for business and analytic purposes, subject to any limitations in the Health Insurance Portability and Accountability Act or other statutory laws relating to privacy and confidentiality that currently exist or exist at any time during the term of this Contract. Anonymized Data means data that has had all County and "Personally Identifiable Information" removed (including, but not limited to, the person's name, address, telephone number, email address, Social Security number of a person etc.) Contractor may share Anonymized Data with third parties for business and analytic purposes. Contractor will not disclose County's Anonymized Data in any manner that would identify County as the source of the data. Neither party will acquire any right, title, or interest in the intellectual property rights owned by the other party by virtue of its performance under this Contract. If any patentable or copyrightable ideas, writings, drawings, inventions, designs, parts, machines or processes are developed as a result of, or in the course of, the work performed under the Contract, including ideas, suggestions or feedback from County (collectively, "Changes"), Contractor shall own all right, title and interest in such Changes.

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

- T. **Compliance with Laws:** Contractor represents and warrants that services to be provided under this Contract shall fully comply, at Contractor's expense, with all standards, laws, statutes, restrictions, ordinances, requirements, and regulations (collectively "laws"), including, but not limited to those issued by County in its governmental capacity and all other laws applicable to the services at the time services are provided to and accepted by County. Contractor acknowledges that County is relying on Contractor to ensure such compliance, and pursuant to the requirements of paragraph "Z" below, Contractor agrees that it shall defend, indemnify and hold County and County Indemnitees harmless from all liability, damages, costs and expenses arising from or related to a violation of such laws.
- U. **Freight:** Intentionally Omitted.
- V. **Severability:** If any term, covenant, condition or provision of this Contract is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remainder of the provisions hereof shall remain in full force and effect and shall in no way be affected, impaired or invalidated thereby.
- W. **Attorney Fees:** In any action or proceeding to enforce or interpret any provision of this Contract, each Party shall bear their own attorney's fees, costs and expenses.
- X. **Interpretation:** This Contract has been negotiated at arm's length and between persons sophisticated and knowledgeable in the matters dealt with in this Contract. In addition, each Party had been represented by experienced and knowledgeable independent legal counsel of their own choosing or has knowingly declined to seek such counsel despite being encouraged and given the opportunity to do so. Each Party further acknowledges that they have not been influenced to any extent whatsoever in executing this Contract by any other Party hereto or by any person representing them, or both. Accordingly, any rule or law (including California Civil Code Section 1654) or legal decision that would require interpretation of any ambiguities in this Contract against the Party that has drafted it is not applicable and is waived. The provisions of this Contract shall be interpreted in a reasonable manner to effect the purpose of the Parties and this Contract.
- Y. **Employee Eligibility Verification:** Contractor warrants that it fully complies with all Federal and State statutes and regulations regarding the employment of aliens and others and that all its employees performing work under this Contract meet the citizenship or alien status requirement set forth in Federal statutes and regulations. Contractor shall obtain, from all employees performing work hereunder, all verification and other documentation of employment eligibility status required by Federal or State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, 8 U.S.C. §1324 et seq., as they currently exist and as they may be hereafter amended. Contractor shall retain all such documentation for all covered employees for the period prescribed by the law. 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 agrees to permit the County's Auditor-Controller or the Auditor-Controller's authorized representative (including auditors from a private auditing firm hired by the County) access during normal working hours to all books, accounts, records, reports, files, financial records, supporting documentation, including payroll and accounts payable/receivable records, and other papers or property of Contractor for the purpose of auditing or inspecting any aspect of performance under this Contract. The inspection and/or audit will be confined to those matters connected with the performance of the Contract including, but not limited to, the costs of administering the Contract. 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 agrees to maintain such records for possible audit for a minimum of three years after final payment, unless a longer period of records retention is stipulated under this Contract or by law. Contractor agrees to allow interviews of any employees or others who might reasonably have information related to such records. Further, Contractor agrees to include a similar right to 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 the County's project manager.

Upon request by Contractor, with reasonable advance notice and conducted in such a manner as to not unduly interfere with County's operations, Contractor reserves the right to audit County's use of the Software to ensure County is in compliance with its usage rights under this Contract. Such audit rights shall survive for a twelve (12) month period following any termination of this Contract.

- 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 DPA in writing when the expenditures against the Contract reach 75 percent of the dollar limit on the Contract. County shall not be responsible for any expenditure overruns and will not pay for work exceeding the dollar limit on the Contract unless an amendment to cover those costs has been executed.

Neither party will be liable for any consequential, special, indirect or exemplary damages or for loss, damage, or expense directly or indirectly arising out of or in connection with the implementation or use of the Software either separately or in combination with any software, data communications or other equipment. Each party's liability for a breach of this Contract shall in no event exceed two times the amount of fees paid under this Contract in the year in which the breach arose except for any breaches of the intellectual property rights indemnification in Paragraph H, Patent/Copyright Materials/Proprietary Infringement, or the confidentiality obligations in Paragraph S, Confidentiality, which are not subject to this limitation on liability.

Additional Terms and Conditions

1. **Scope of Contract:** This Contract specifies the contractual terms and conditions by which Contractor shall provide Employee Health Software Solution System to County, as further detailed in Attachment A, Scope of Work.
2. **Term of Contract:** This Contract shall commence on **January 1, 2024 , through and including December 31, 2026**. The Contract shall be in effect for the time periods specified unless this Contract is earlier terminated by the Parties. The Contract may be renewed for two (2) additional one (1) year periods upon the Parties' mutual agreement. County does not have to give reason if it elects not to renew. Renewal periods may be subject to approval by the County of Orange Board of Supervisors.
3. **Breach of Contract:** The failure of Contractor to comply with any of the provisions, covenants or conditions of this Contract shall be a material breach of this Contract. In such event, County may, and in addition to any other remedies available at law, in equity, or otherwise specified in this Contract, do any of the following:
 - a) Terminate the Contract immediately 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 above.
4. **Civil Rights:** Contractor attests that services provided shall be in accordance with the provisions of Title VI and Title VII of the Civil Rights Act of 1964, as amended, Section 504 of the Rehabilitation Act of 1973, as amended; the Age Discrimination Act of 1975 as amended; Title II of the Americans with Disabilities Act of 1990, and other applicable State and federal laws and regulations prohibiting discrimination on the basis of race, color, national origin, ethnic group identification, age, religion, marital status, sex or disability.
5. **Conflict of Interest – 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 Key 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 the County's Project Manager, which consent shall not be unreasonably withheld.

The Contractor's Project Manager shall be assigned to this project for the duration of the Contract and shall diligently pursue all work and services to meet the project time lines. The County's Project Manager shall have the right to require the removal and replacement of the Contractor's Project Manager from providing services to County under this Contract. The 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 the County's Project Manager. The County's Project Manager shall review and approve the appointment of the replacement for the Contractor's Project Manager. County is not required to provide any information, reason or rationale in the event it requires the removal of Contractor's Project Manager from providing further services under the Contract.

7. **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).

8. **Debarment:** To the extent applicable, Contractor certifies that neither Contractor nor its employee(s) are presently debarred, proposed for debarment, declared ineligible or voluntarily excluded from participation in a contractual transaction by any state or federal department or agency. County may terminate this Contract if Contractor is or becomes subject of any debarment, pending debarment, declared ineligibility or voluntary exclusion from participation by any state or federal department or agency.

9. **Cooperative:** Intentionally Omitted.

10. **Disputes – Contract:** Intentionally Omitted.

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

1. Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited and

specifying actions to be taken against employees for violations, as required by Government Code Section 8355(a)(1).

2. Establish a drug-free awareness program as required by Government Code Section 8355(a)(2) to inform employees about all of the following:
 - a. The dangers of drug abuse in the workplace;
 - b. The organization's policy of maintaining a drug-free workplace;
 - c. Any available counseling, rehabilitation and employee assistance programs; and
 - d. Penalties that may be imposed upon employees for drug abuse violations.
3. Provide as required by Government Code Section 8355(a)(3) that every employee who works under this Contract:
 - a. Will receive a copy of the company's drug-free policy statement; and
 - b. Will agree to abide by the terms of the company's statement as a condition of employment under this Contract.

Failure to comply with these requirements may result in suspension of payments under the Contract or termination of the Contract or both, and 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.
12. **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.
 13. **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.

14. **News/Information Release:** Contractor agrees that it will not issue any news releases in connection with either the award of this Contract or any subsequent amendment of or effort under this Contract without first obtaining review and written approval of said news releases from County through the County's Project Manager.
15. **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 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:	Cority Software, Inc.
	Attention:	General Counsel
	Address:	9 th Floor, 250 Bloor Street East Toronto, ON M4M 1E6
	Telephone:	281-221-9687
	E-mail:	notices@cority.com
For County:	Name:	County of Orange HCA/Purchasing
	Attention:	Roland Tabangin
	Address:	405 W. 5 th Street Suite 600 Santa Ana, CA 92701
	Telephone:	(714) 834-3181
	E-mail:	rtabangin@ochca.com
CC:	Name:	County of Orange HCA
	Attention:	Stephanie Plowman
	Address:	600 W. Santa Ana Blvd. Suite 405

Santa Ana CA 92701
 Telephone: 714-565-3780
 E-mail: splowman@ochca.com

16. **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.
17. **Termination – Orderly:** After receipt of a termination notice from the County of Orange, Contractor may submit to the County a termination claim, if applicable. Such claim shall be submitted promptly, but in no event later than 60 days from the effective date of the termination, unless one or more extensions in writing are granted by County upon written request of Contractor. Upon termination, County agrees to pay Contractor for all services performed prior to termination which meet the requirements of the Contract, provided, however, that such compensation combined with previously paid compensation shall not exceed the total compensation set forth in the Contract. Upon termination or other expiration of this Contract, each party shall promptly return to the other party all papers, materials, and other properties of the other held by each for purposes of performance of the Contract.
18. **California Public Records Act:** Contractor and County agree and acknowledge that all information and documents related to the award and performance of this Contract are subject to disclosure pursuant to the California Public Records Act, California Government Code Section 7920 et seq.
19. **Gratuities:** Contractor warrants that no gratuities, in the form of entertainment, gifts or otherwise, were offered or given by Contractor or any agent or representative of Contractor to any officer or employee of County with a view toward securing the Contract or securing favorable treatment with respect to any determinations concerning the performance of the Contract. For breach or violation of this warranty, County shall have the right to terminate the Contract, either in whole or in part, and any loss or damage sustained by County in procuring on the open market any goods or services which Contractor agreed to supply shall be borne and paid for by Contractor. The rights and remedies of County provided in the clause shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.
20. **Parking for Delivery Services:** County shall not provide free parking for delivery services.
21. **Software – Maintenance:** Contractor will provide telephone support to the County's end-users and technical support staff 24 hours per day from Monday to Friday excluding Christmas Day (December 25th), Boxing Day (December 26th), and New Year's Day (January 1st). Prior to using Contractor's telephone support services, County's end-users are expected to have a reasonable familiarity with the Software either through formal training provided by Contractor or the equivalent in informal training provided by County's staff. End-user telephone support is for the purpose of responding to possible errors in the Software or set-up of the Software and other issues of a technical nature, including but not limited to issues arising out of County's hardware and operating systems compatibility with Contractor's software. The correction of any residual errors in any software products

after implementation which may be discovered by Contractor or by County shall be considered maintenance. Such maintenance shall be performed by Contractor without additional charge for the duration of this Contract. Telephone support does not include implementation service, programming, or resolution of County's computer system problems that are unrelated to the operation of the Software, but does include assistance with report generation.

22. **Software License:** Contractor hereby grants to County of Orange and County accepts from Contractor, subject to the terms and conditions of this Contract, a non-exclusive, global, non-transferable (except as provided in this Contract) license to use Contractor's software identified in this Contract, including updates, upgrades, enhancements, improvements, and modifications to which the County is entitled pursuant to the terms of this Contract (the "Software")., in object code format (and related documentation) for use on the County's database and on computer systems having the minimum system requirements and including the right to make such additional copies of the Software as necessary for archive, testing or backup purposes. For the purpose of this Contract, Updates mean changes or patches to be integrated with the Software to correct errors and that do not alter the functionality or the content of the Software.
23. **Software – Acceptance Testing:** Acceptance testing may be required as specified for all Contractor-hosted software as specified and listed in the Contract or order. Included in this clause are improved versions, including new releases, of this Software, any such software which has been modified by Contractor to satisfy County requirements, and any substitute software provided by Contractor in lieu thereof, unless the Contract or order provides otherwise. The purpose of the acceptance test is to ensure that the software operates in substantial accord with Contractor's technical specifications and meets County's performance specifications.
24. **Software – Future Releases:** If improvement, upgraded, or enhancement versions of any software product under this Contract are developed by Contractor and are made available to other licensees, they shall be made available to County at County's option, provided such versions are operable on the same computer hardware configuration.

25. **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.

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 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.

Rafael Linares Chief Information Security Officer 1055 N. Main St, 6th Floor Santa Ana, CA 92701 Office: (714) 567-7611 E-mail: Rafael.linares@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.

26. **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.

27. **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.
28. **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.
29. **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.
30. **No Third-Party Beneficiaries:** This Contract is a 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.
31. **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)

RESOLUTIONS of the Board of Directors
of Cority Software Inc. (the "**Corporation**")
passed effective the January 8, 2020.

1. APPOINTMENT OF CHIEF REVENUE OFFICER

Be it resolved that:

Stephen Molen is appointed to the position of Chief Revenue Officer ("CRO"), effective as of January 1, 2020.

2. APPOINTMENT OF OFFICERS

Be it resolved that:

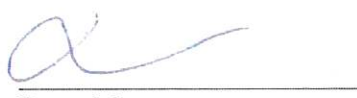
The following persons are appointed officers and signing authorities of the Corporation to hold the offices referred to below opposite their respective names until a successor is appointed by resolution of the Directors:

Mark Wallace	President and CEO
Stan Marsden	Executive Vice President and Chief Technology Officer
Ryan Magee	Chief Financial Officer and Secretary
Michael Couture	Chief Product Officer
Stephen Molen	Chief Revenue Officer
Pablo Neiman	Vice President, Professional Services

The undersigned, being the directors of the Corporation, hereby consent to the above-noted resolutions pursuant to the provisions of the *Business Corporations Act*, British Columbia.



Mark Wallace



Ryan Magee

SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties hereto have executed this Contract No. MA-042-24010451 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: Cority Software, Inc.

Stephen Molen

Chief Revenue Officer

Print Name

Title

Signature

DocuSigned by:

 5588EDE7A86E4BB...

11/10/2023

Date

Ryan Magee

Chief Financial Officer

Print Name

Title

Signature

DocuSigned by:

 F4222773AD42480...

11/10/2023

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

Deputy County Counsel

Print Name

Title

Signature

DocuSigned by:

 9713A4061D4343D...

11/12/2023

Date

ATTACHMENT A

SCOPE OF WORK

A. BACKGROUND

The Orange County Employee Health Services (EHS) department provides an array of services to help ensure that all Orange County (OC) employees are as fit and healthy as possible to perform their job duties effectively and without risk to their own or others' health and safety. OC's work force consists of approximately 18,000 employees, contractors, volunteers and interns from over 20 Agencies. The Agencies include but are not limited to the OC Sheriff-Coroner Department, John Wayne Airport, OC Waste and Recycling, OC Social Services, OC Health Care Agency, OC Probation, OC District Attorney, OC Public Works, and central administrative areas such as Human Resources, Risk Management, Procurement, etc.

B. OBJECTIVE

The software application to be provided by Contractor includes functional support for all services as noted below. This Contract includes licenses for use of the software application, routine support and maintenance services, and professional services for ongoing software customization, project management and training to staff. Details related to each of these is noted below. This application is referred to as OC Employee Health Management System (EHMS).

C. SYSTEM COMPONENTS AND FUNCTIONALITY

The software application must support all functional areas of responsibility under EHS. This includes:

Pre-placement and ongoing annual physical/medical examinations of all workforce members, including professional services contractors.

Medical surveillance examinations for all applicants and workforce members. All groups need to be reviewed for correct exam components, SEG groups, letters etc.

1) Hazardous Materials (HazMat) Module

- a) Include Hazardous Materials Questionnaire (HMQ), Pre-Placement Examination (PPE) Questionnaire, audiogram, Pulmonary Function Test (PFT), Stress EKG, lab work, section for documenting Chest X-Ray (CXR) results, import physical test.
- b) Ability to configure testing requirements by job role or title and to define protocols for different employee groups.
- c) Create notifications and alerts one (1) month prior to examination due date and send notification to employee by email. Notification shall be modified by EHS to meet specific examination needs.

2) Asbestos Examination Module

- a) Available to any workforce member identified by department or Industrial Hygiene as having the potential for occupational exposure to asbestos or asbestos-containing material.
- b) Ability for the Asbestos Medical Initial and Annual questionnaire (AMQ-I or AMQ-A) to be available electronically for completion and submission.
- d) Ability to configure testing requirements by job role or title and to define protocols for different employee groups.
- c) Include Respirator Certification (RC), PFT, audiogram, and lab work.
- d) Identify need for an initial exam by job title and notify employee by email for subsequent examinations one (1) month prior to examination due date.
- e) Select appropriate examination components based on age or year since first exposure.

3) SCUBA Examination Module

- a) Available to employees identified as potential or current members of the OCSD Dive Team prior to job assignment, annually, after an illness or injury requiring hospitalization of more than twenty-four (24) hours, and after an episode of unconsciousness related to diving activity.
- b) Ability to input Stress EKGs performed initially and then annually for those over 35 years of age.
- c) Ability to configure testing requirements by job role or title and to define protocols for different employee groups.
- d) Select appropriate examination components based on age or year since first exposure.

4) Respirator Medical Examination/Fit Testing Module

- a) Ability to configure testing requirements and to define protocols for different workforce subgroups.
- b) Ability to input mask make, model and size.
- c) Ability to accept electronic results from various OSHA approved fit testing machines.
 - d) Establish healthcare locations for offsite mobile events to link to billing module.
- e)

5) Lead Examination Module

- a) Employees shall have the ability to either access the EHMS to enter data (medical history questionnaire, lead surveillance questionnaire), or the EHMS shall have the ability to accept data from external sources (scanned forms or imported data).
- b) Ability to configure testing requirements by job role or title and to define protocols for different employee groups.
- c) Ability to identify need for an initial exam by job title sub-group.
- d) Ability to notify employees by e-mail for subsequent examination one (1) month prior to examination due date.
- a) Produce cumulative examination reports with lead results on each employee/department for past five (5) years.
- b) Select appropriate examination components based on initial or annual examination.

6) Federal Aviation Administration (FAA) Examination Module

- a) Available to employees identified by OCSD Human Resources or Safety Officer as pilots, who require second-class commercial certification prior to entry into the group and on a biennial basis.
- b) Ability to support FAA History (FAA-H) and FAA Physical (FAA-P) forms obtained from FAA examining physician, audiogram, vision testing, urinalysis, pulse, blood pressure, and a baseline EKG at age 35 then annually at age ≥ 40 .
- c) Ability to configure testing requirements by job role or title and to define protocols for different employee groups.
- d) Ability to configure for an initial examination by job title.
- e) Ability to notify employees by e-mail for subsequent examinations one (1) month prior to examination due date.

7) Hazardous Device School (HDS) Examination Module

- a) Ability to support HDS History and physical forms provided to the employee by the Department of Justice (DOJ), urinalysis, audiogram, body fat testing, vision testing, EKG, and PFT test if indicated.
- b) Available to employees identified by OCSD Human Resources or department as Bomb Squad.
- c) Ability to configure testing requirements by job role or title and to define protocols for different employee groups.

8) Crane Operator Module

- a) Ability to configure testing requirements by job role or title and to define protocols for different employee groups.
- b) Available to employees identified by their department as Crane Operators.
- c) Include the Physical Examination from the National Commission for the Certification of Crane Operator.

9) DMV Examination Module

- a) Ability to configure testing requirements by job role or title and to define protocols for different employee groups.
- b) Available to employees identified by their department as requiring a class B DMV license in order to perform their duties.

10) Hearing Conservation Medical Surveillance (HCMS) Module

- a) Ability to configure testing requirements by job role or title and to define protocols for different employee groups.
- b) Ability to enter results of audiometric testing for potential standard threshold shifts and refer employees for additional audiometric testing if needed.
- c) Ability to create a report of and forward all audiometric results to an outside audiologist for final determination.
- d) Notify employees by e-mail for subsequent examinations due.

11) Appointment Scheduling Module

- a) Automatic "appointment reminder" feature that reminds the employees and applicants of their upcoming appointment at EHS offices, worksite mobile field locations or at County's contracted provider locations. Send Microsoft Outlook email notifying the employees and applicants of their appointment date and time.
- b) Ability to print selected calendar information.

12) Blood borne Pathogen Module

- a) Data entry screen shall include the following fields: exposed employee's name, Employee ID number, supervisor filling out form, supervisor's phone number, date and time of incident, type of injury, type of body fluid, name and date of birth of source person, source identification number or booking number, name of designated Workers' Compensation clinic.
- b) Ability to manually create records for non-County employees, with the following data elements: name of person, occupation, personal phone number, name of employer, work phone number, date and time of incident, scanned copy of all documents sent by fax or email, type of injury, type of body fluid, name of

healthcare provider treating exposed employee, source lab test results, entity performing source lab tests.

- c) Ability to enter exposure events on a work list until lab results are received by authorized clinicians. Allow clinicians to send email to employee and/or supervisor reporting exposure.

13) Billing Module

- a) Track services ordered and performed by EHS and contract providers at various rate schedules including bundled rates for some providers.
- b) Validate if the services are completed by EHS or County's contractors, if completed onsite at EHS or offsite at a mobile clinic.
- c) Apply the respective cost for services/procedures completed at EHS, at mobile clinics and County's contract clinics.
- d) Have a modifiable table listing the description of all available services and the associated costs with variable pricing tables per vendor and per services.
- e) Ability to track the status of the employee/applicant from the time services are scheduled to when the encounter is closed.
- f) Print forms and employee/applicant labels (auto-generated from profile) from the application.
- g) Ability to create a reconciliation spreadsheet for what was ordered versus what was completed.
- h) Generate invoices for the various agencies. Invoice can be configured by date range and other specified variables.
- i) Billing encounter shall include location where services provided, service date, description of service ordered, charge amount corresponding to services, quantity of services, and free form text field.

14) Fitness for Duty Evaluations

- a) When requested by County Agency Human Resources representative or other designee, provide appropriate referral for Fitness for Duty Evaluation to determine the employee's fitness to perform their work duties.

15) Vaccine administration

- a) Provided to applicants and employees identified by their job title, or California Code of Regulations Title 8, Section 5193, or communicable disease exposure notification. Must be tracked for worksite locations through mobile EHS field services and linked to billing module.
- b) Must have recall programming ability, based on various vaccine types, booster doses, multiple doses for series completion in order to launch notice to employees of upcoming due dates one month in advance.

16) Tuberculosis Occupational Exposure and Notification

- a) Provided to employees identified by the TB Controller with a potential occupational TB exposure incident, and to employees identified by the department/agency to be at risk for occupational TB exposure. This includes configuration for the delivery of exposure notifications to SEG groups, questionnaire link, SEG group recall for subsequent exposure notifications and testing if warranted.
- b) Create reports for departments and exposure groups to include employee name and last TB date. Create reports based on information from questionnaires, TB test results, chest x-ray (CXR) results, conversion data, and referral for further treatment.

17) Communicable Disease Exposure (CDE) Examination

- a) Create notifications and alerts two (2) weeks prior to vaccine dose or follow-up appointment and send notifications to employee by email. Ability to send modifiable notification memos to exposed employees by email.

18) Airborne transmissible disease (ATD) exposure follow up

- a) Provided to employees exposed to airborne pathogen communicable diseases in the course of their duties. Treatment may be provided by EHS, a Worker's Compensation provider, or the employee's primary physician.

19) Employee COVID Contact Tracing, exposure notification and follow-up.

- a) Layout support to maintain efficiency and process consolidation for COVID cases.
- b) Support for audit procedures in Contractor for launching exposure notifications to employees.

20) Employee COVID outbreak and exposure testing

- a) COVID Vaccine Administration Module
 - o Create notifications and alerts two (2) weeks prior to next due vaccine dose or follow-up appointment; and send notification to employee by email.
 - o Ability to import all current vaccine information statements (VIS) from the CDC.
 - o Interface with state California Immunization Registry (CAIR) website for vaccine data lookup and data feed of employee vaccines administered.

21) Employee MyCority Dashboard vaccine record lookup

- a) Create modifications to the current employee COVID vaccine and mandate dashboard to allow employees to view other types of vaccine records submitted to EHS in their Health Record
- b) Create a request for vaccine records from the Employee Dashboard for employees to make these requests.

- 22) Work Classification/ Title Schematic review and updates
- 23) Mobile Occupational Health Services
- 24) EHS Consultative Services
- 25) Support for surveys
- 26) Ongoing compliance with regulatory requirements, including those related to COVID-
- 27) Pre-defined and support for adhoc reports and dashboards, and data extracts to support visibility and analysis of all data. Activities shall include:
 - a) Produce reports using specific attributes, e.g., agency, department, employee name, employee ID, most recent examination date, next due date, overdue examinations, complete or incomplete examinations, total number of examinations completed per agency and/or department per year, laboratory tests, vaccines, medications, illnesses, medical standard, exposure group identification number. Sort by agency and/or department.
 - b) Generate statistical reports and merge duplicate records as needed.
 - c) Generate reports of Contractor user types and inactivity, consolidate unused users and remove duplicate users such as applicants that have become employees or separated employee users no longer requiring access, in order to maintain the accuracy of applicable user licenses for this contract.
 - d) Ability to generate a report that tracks the life cycle of any encounter. This could include total elapsed days of completed encounters and / or a list of current incomplete encounters.
 - e) Ability to run pre-defined and ad-hoc reports with services and procedures rendered.
 - f) Standard reports shall be accessible to end users. Contractor and County shall define and customize standard reports during Application implementation and throughout the term of this Contract.

The application shall be able to create reports that include, but are not limited to, the criteria/ parameters listed below:

OCCUPATIONAL EXPOSURES
<ul style="list-style-type: none"> • Blood-Borne Pathogens (BBP) • Airborne Transmissible Diseases (ATD)
BBP – Aggregate Count of Employees who sustained a BBP Exposure
<ul style="list-style-type: none"> • By Agency and by Department • By Month and by Year or any selected time frame
BBP – Count by Type of Exposure

<ul style="list-style-type: none"> • By Agency and by Department • By Month and by Year or any selected time frame <ul style="list-style-type: none"> ○ Percutaneous ○ Mucus membrane ○ Cutaneous with non-intact skin
BBP – Elapsed Time from Initial EHS Notification to Time EHS Initiated Action <ul style="list-style-type: none"> • By Agency and by Department • By Employee Name and Employee ID
ATD – Immunity to Specified Disease <ul style="list-style-type: none"> • By incident • By Agency, Department, Location, and/or Job Title • Vaccination status • Titer status
ATD – Count of specific event <ul style="list-style-type: none"> • By Agency and by Department • By Month and by Year or any selected time frame
ATD – List of Employee Names and Employee ID <ul style="list-style-type: none"> • By Event, by Agency and by Department • By work location • By date or date range
ATD – List of Follow Up Actions <ul style="list-style-type: none"> • By employee and Employee ID • Indication if Complete or Incomplete
ATD – List of Employee Names with Respirator Fit Testing information <ul style="list-style-type: none"> • Brand of mask • Type of mask • Size of mask
ATD – List of communicable disease exposure events <ul style="list-style-type: none"> • By date • By disease • By agency/department
ATD – List of Employee Names and Date of Last Fit Test <ul style="list-style-type: none"> • By Agency and by Department
FINANCIAL
Total Costs <ul style="list-style-type: none"> • By Agency and by Department • By Month and by Year or any selected time frame
Procedure and Service Costs <ul style="list-style-type: none"> • By procedure / service description • By Employee • By Encounter
Invoices for services performed <ul style="list-style-type: none"> • By date, month, type of service • By service location (EHS, contract clinic) • By agency/department
Statistical reports of services performed

<ul style="list-style-type: none"> • By location (EHS, contract clinic, mobile services) • By date or date range • By agency/department • By specific EHS provider • By specific EHS clerical staff member
DEMOGRAPHICS
Count of Employees <ul style="list-style-type: none"> • By County, by Agency and by Department • By job title
Age Distribution of Employees <ul style="list-style-type: none"> • By County, by Agency and by Department
Import changes <ul style="list-style-type: none"> • By date, lists changes to demographic information imported from CAPS+
Home address <ul style="list-style-type: none"> • Print label or envelope based upon employee/applicant home address
PRE-PLACEMENTS
IMMUNIZATIONS
<ul style="list-style-type: none"> • Aggregate count of Employees who require vaccines • By type (pre-employment, exposure, or offers of non-required vaccines) • By agency and department • By employee name, date of birth or Employee ID • By date range • By type of vaccine received • By results (number of employees who received an optional vaccine for example) • By exposure date
MEDICAL SURVEILLANCE EXAMINATION REPORTS
<ul style="list-style-type: none"> • Aggregate Count of Employees who require a medical surveillance exam • By type of exam • By agency and department • By employee name, date of birth, Employee ID • By date range
TUBERCULOSIS SCREENING
<ul style="list-style-type: none"> • Aggregate count of Employees who require Tuberculosis screening • By type of exam • By agency and department

- By employee name , date of birth, Employee ID
- By date range
- By type of test received
- By results including last result and results over time
- By exposure date
- By TB status (previous positive, negative, etc.)
- By receipt of recommended screening (Questionnaire, TB skin test, CXR)
- Notification memos to group
- Notify exposure group by e-mail when second test is due and continue to notify at set interval until complete
- Ability to calculate conversion data

- 28) Support and maintenance of patient demographics information
- 29) Support for access management controls such as roles and audit logs
- 30) Support for mobile field-based access
- 31) Ensure complete integration with the County CAPS+ database for all agencies, and others as needed.
- 32) Support all mandated data exchange and interface requirements, such as CAIR.
- 33) Enable specific attributes to be added to job titles, e.g., exam name and time intervals.
- 34) Support visual color coding to differentiate blocked times from available times in scheduling platform.
- 35) Retain historical information for staff 30 years after employee separates from County.
- 36) Provide approved managers the capability to review compliance related items with respect to subordinate staff.
- 37) Support the use of unique identifiers for tracking services performed for employees and new applicants at different locations.
- 38) Contractor shall complete the development of, maintain and configure all assessments and database field customizations for the application.
- 39) Contractor shall establish all assessments and database field customizations for all applications that will interface with the EHMS. Contractor shall also provide the setup, configuration and maintenance of data collection and reporting for the application.

D. Professional Services

Contractor shall provide development support and training services, which include objectives such as:

- 1) Optimize the use of the application to accommodate fluctuations and changes related to COVID-19 management.
- 2) Support all current and ongoing changes and optimizations to all of the modules as necessary.
- 3) Business intelligence, reports and dashboards training.
- 4) Assistance with additional module configuration, workflow review and optimization, list and layout configuration, scored questionnaires configuration, form mapper configuration, and advance business rules configuration.
- 5) Cority consultant must be Senior Consultant

E. Software License, Support and Maintenance

- 1) Contractor shall provide the agreed number of administrative licenses to County set forth in Attachment B, Fees and Charges. Such licenses are subject to the terms of this Contract and any other provision or other 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.
- 2) Contractor shall provide the agreed number of end user Portal licenses to County set forth in Attachment B, Fees and Charges -.
 - a) County's end users shall only use the application for the purpose intended and authorization for access shall be determined and managed by County. Unauthorized use shall include, but not be limited to (i) using the Application to provide data processing services to any unauthorized/third-party persons, (ii) making copies of the Application for distribution to third parties, and (iii) reverse-engineering or decompiling the Application for the purpose of designing or developing a system competitive with Contractor's Application.
 - b) Contractor shall provide Application support and routine maintenance including entitlement to new releases and versions generally released by the Contractor and complete database access by County staff for any data extracts, reporting or maintenance.
 - c) County shall be responsible for ensuring that only authorized end users access the Application.
 - d) Any custom development or enhancement of the application commissioned by and paid for by the County shall remain the intellectual property of the County.
 - e) Data Ownership
 - o Contractor shall establish and maintain a source code escrow, and County shall have access to the source code in the event of bankruptcy, dissolution, merger or other situation that may impact Contractor's ability to support

Contractor's Application. All County data in the Application shall remain the property of County.

- f) Data Extraction
 - o Upon termination or expiration of this Contract or cessation of business by Contractor or other event preventing Contractor from continuing to perform under this Contract or in the event the Contractor undergoes a bankruptcy, dissolution, merger or other situation that may impact Contractor's ability to support Contractor's Application, Contractor will export data from the application in a useable data format approved by County, as well as the data dictionary and all related information to facilitate continued use.
- a) At any time during the term of this Contract, County shall be able to extract County data from the Application without cost, contingencies, conditions, policies or technical barriers.
- b) Contractor shall not withhold County data or refuse for any reason, to promptly return to County all County data (including copies thereof) if requested to do so on such media as reasonably 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.

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

F. TECHNOLOGY REQUIREMENTS AND OBJECTIVES

- 1) The application shall support and satisfy all provided County and HCA IT security requirements, noted in Attachment D.
- 2) Support for bi-directional data exchange and necessary interfaces to and from other relevant systems, either through direct linkages or via the use of compliant interoperable API standards and methods.
- 3) All changes and updates to the application shall follow standard change management protocols, including timely communication, impact analysis, documentation, implementation schedule, support during implementation and resolution of issues, and ongoing support for customized functional solutions and enhancements.
- 4) Field based mobile access must support laptops on Windows operating system, and iPads in the native Apple operating system. The application's performance, look-and-feel, visual scaling and flow shall be consistently identical to the extent possible on all platforms.
- 5) The application shall be optimized for performance based on internet connection speed and quality when used in the field.

b. Contractor Support Responsibilities

Contractor responsibilities shall include all or part of the following tasks as required by County and agreed by Contractor.

- 1) Work with HCA IT staff in monitoring the performance and connectivity whenever there are issues relating to the Application.
- 2) Maintain the required 99.9% optimal availability by ensuring timely correction of all EHMS infrastructure problems and monitoring and responding to application console messages.
- 3) Monitor and maintain the integrity and accuracy of all data.
- 4) Configure, test, and fine-tune the application on a continuing basis.
- 5) Work collaboratively with the HCA Change Advisory Board (CAB) to ensure that all changes are documented and approved prior to implementation.

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

- 6) 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.
- 7) NIST. To ensure compliance with HIPAA, Application Service Providers shall implement appropriate security safeguards by following National Institute of Standards and Technology (NIST) guidelines.

G. SERVICE LEVEL AGREEMENT

The table below outlines County's minimum requirements to respond to issues based upon priority levels.

Severity Levels	Issue	Response	Resolution
Severity 1	a) The entire system is non-functioning. b) County or Public users are unable to complete workflows and no workarounds are available.	Contractor shall respond to the notification within one hour.	Immediate resolution within four hours of initial report. Status reports are required hourly during this period until resolved.

Severity 2	a) Inability to use system with some limitations of features or service that is normally provided. b) System failure impacting some workflows and users.	Contractor shall respond to the notification within one hour.	Resolution within 24 hours of initial report.
Severity 3	a) Major operational impact, even if workarounds are available.	Contractor shall respond to the notification within four hours.	Up to 3 days to provide resolution.
Severity 4	a) Issue is cosmetic in nature and has no impact on functionality or accessibility. b) A new request, report, or functionality.	Contractor shall respond to the notification within 24 hours.	Up to 5 days to provide resolution/response.

Maintain the application's uptime and full availability at 99.9%.

H. User Training Requirements

County shall approve Contractor's training plan if it varies from the proposed plan below. Initially staff members shall require "classroom led" hands on training; Super Users shall provide training to staff on an as needed basis after full implementation. In addition to the training requirements identified herein, it is expected that Contractor shall provide training for all the future functionality provided by the Application, including third party contractors provided by Contractor or County.

The training shall be broken down into four (4) major groups: End User, Super User, Software Support, and Ad Hoc Report Training – See below:

a) End User Training

End Users are the largest group in need of training. They are further broken down into more specific groups based upon their job function, logon group, and access rights. This includes training for new releases.

b) Super User Training

A "Super User" will be a staff member with good overall working knowledge of computers and EHS that will assist application users with general computer and application problems and will be able to generally distinguish between hardware, operating system, network, and application errors. If Level Zero (0) is unable to resolve the problem, it will be referred to the Level One (1) Service Desk. This includes training for new releases.

c) Software Support Training

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 and technical level training.

Software support staff must be able to recognize core issues, versus issues that can be cured with a work around. Software Support shall be charged with testing of new releases and updates.

d) Ad Hoc Report Training

The application shall have the ability to do Ad Hoc reporting. Many of the reports that the staff may need shall be incorporated into the application and made available simply by selecting them. Since the new application shall have a built in report generator, some staff members shall have access to use the Ad Hoc reporting tools. For these users, it shall be necessary to provide training in the use of the Ad Hoc report generator.

I. Documentation Requirements

1) Application User Documentation

Contractor shall provide the following:

- a) How to enter data into the application, track status of a request, find data already entered,
- b) Generate reports appropriate to their group rights.
- c) How to verify if a user has lost a connection to the application.
- d) How to troubleshoot minor installation issues.
- e) Perform standard and advanced searches and to generate reports appropriate to group rights.
- f) Interface troubleshooting.
- g) How to upload/attach documents into the application.
- h) How to create ad hoc reports.
- i) How to create and modify look up tables and add/inactivate a list item.
- j) Find lost records.
- k) Delete duplicate records.
- l) Troubleshoot locked records.

2) Super User Documentation

Contractor shall provide Super Users with the following:

- 1) Perform standard and advanced searches and to generate reports appropriate to their group rights.
 - 2) Troubleshoot lost connections to the application/server.
 - 3) How to check print queues.
 - 4) Advanced reporting features.
 - 5) Interface troubleshooting.
 - 6) Delete duplicate records.
 - 7) Administrative User Documentation.
- a. All technical specifications, design, troubleshooting techniques, data dictionary, application logic. Everything that a typical admin does.

J. Project Management

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

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

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 application failure. The escalation procedures shall require approval of County Project Manager. The escalation procedures shall include, but not be limited to the following:

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

1) HCA Design & Implementation Work Plan

1) Develop Project Plan

Contractor shall provide 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 with HCA approval as needs may dictate.

Contractor shall provide the project plan to County for approval prior to initiating any tasks. Contractor shall maintain an up-to-date version of the work plan using Microsoft Project or other software as approved by HCA. All changes to deliverable time frames that impact major milestones must be approved at least two (2) weeks prior to the milestone, in writing, by County's Project Manager. All approved changes shall be reflected in the work plan and Contractor shall highlight and explain any major changes to an earlier approved version.

Contractor shall identify all relevant assumptions made in the development of the project plan, and upon which the estimates have been calculated must be clearly documented, including assumptions made for development software tools, use of any third party software, and HCA resources providing assistance.

2) Conduct Joint Application Design to Confirm Requirements

Contractor shall lead and conduct Joint Application Design (JAD) or similar facilitated requirements and analysis design sessions with HCA staff and other stakeholders which may be identified by HCA. The purpose of these JAD is to confine and update HCA view of EHS functional requirements, features and capabilities, technology requirements and interface requirements, and to provide Contractor an opportunity to perfect its understanding of HCA environment and programs. The JAD shall also document high level workflow within EHS to identify potential changes in EHS workflow design or in HCA workflow, policies and procedures.

Contractor shall document the updated EHMS, interface and other requirements. Contractor shall document the results of its JAD sessions using a structured analysis and design methodology as approved by HCA IT. The resulting document shall be presented in a walkthrough and must be approved by HCA.

3) Development, Testing & Training Environments

Contractor shall have separate development, testing, and training environments for the EHMS development accessible to HCA IT staff. EHS staff shall also have access to these environments for monitoring Contractor work, validating test results, and other reasons as needed.

4) Develop Application Specifications Document

Contractor shall develop an Application Specifications Document which identifies the changes necessary to Contractor's existing application code to provide any new or modified functionality.

5) Customize & Configure Core Application Software

Contractor shall modify all program code for COTS application to reflect EHS requested customizations.

6) Interface Development

Contractor shall fully develop and test any defined interfaces between the EHMS and any internal and external applications which are included in the approved application requirements document.

7) Unit Testing

Contractor shall perform iterative unit testing as program code is developed to ensure that the code works as required. Contractor shall create test plans documents for all use cases.

8) Unit Test Code Corrections

Contractor shall make corrections to code based on unit test results.

9) Integration & Regression Testing

Successfully Regression testing must be completed and signed off by users for final acceptance of product.

10) Application Test

Contractor shall test the integrity and responsiveness of the application A and its capacity to support the EHMS. The test must include application response time testing, application feature testing, regression testing, throughput, configuration sizing, and bottleneck identification. Any application-related problems identified must be discussed and resolved in conjunction with HCA IT.

11) User Acceptance Testing

Contractor shall conduct a User Acceptance Test to ensure that HCA users are able to successfully use the EHMS and that all modified workflows, policies and procedures are consistent with it. Contractor shall develop test scripts and data for this test, review the results and recommend initial application acceptance. HCA users shall assist in the actual test and shall be responsible for final approval of user acceptance test recommendations.

ATTACHMENT B**COMPENSATION AND INVOICING****1. Compensation**

This is a fixed price Contract not to exceed the amount of \$378,742.50 for the Term of Contract.

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

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

A. Annual Software Subscription Cost Per Year:

	Solution	Units	Pricing (USD)
1.	100: Occupational Health Suite: 1-9 users	9	23,123
2.	100: Occupational Health Suite: 10-19 users	6	14,337
3.	MyCority		10,000
4.	Cority Hosted Integration(s)		6,000
5.	Monthly Processing		-
6.	Weekly Processing		-
7.	Daily Processing		-
8.	Multiple Times per Day Processing		-
9.	User – Administrator (IT Administrators)	5	12,847.50
10.	Data Storage	90	10,660
11.	Users – Employee	30000	16,000
			-
	Total		92,967.50

B. Annual Consulting Fee Per Year:

Maximum Annual Professional Services Hours/Days	Annual CAP Fee (\$)
160 hours	\$33,280

1. County may use the professional services time set out above for Training and Enablement Services by making a request in writing to Contractor.
2. A resource from Contractor Professional Services will be assigned to complete the requests within the timeframes outlined below:

Requests for on-site consulting (a minimum of 24 consulting hours over 3-consecutive days will be required for onsite work); On-site time, consultants travel time, and travel expenses will be billed to the Client. Travel time will be billed at 50% of the consulting rate. Travel costs will be billed as incurred or in accordance with the daily per-diem rate.	4 weeks
Requests for remote consulting for partial days	2 business days
Requests for remote consulting for full days	5 business days

3. **Price Increase/Decreases:** No price increases will be permitted during the first period of the Contract. . A minimum of 30-days advance notice in writing is required to secure such adjustment. No retroactive price adjustments will be considered. The County may enforce, negotiate, or cancel escalating price Contracts or take any other action it deems appropriate, as it sees fit. The net dollar amount of profit will remain firm during the period of the Contract. Adjustments increasing the Contractor's profit will not be allowed.
4. **Firm Discount and Pricing Structure:** Contractor guarantees that prices quoted are equal to or less than prices quoted to any other local, State or Federal government entity for services of equal or lesser scope. Contractor agrees that no price increases shall be passed along to the County during the term of this Contract not otherwise specified and provided for within this Contract.
5. **Contractor's Expense:** The Contractor will be responsible for all costs related to photo copying, telephone communications and fax communications while on County sites during the performance of work and services under this Contract.
6. **Payment Terms:**

Payment for annual software subscription: Payment shall be made in advance within 30 days after receipt of an invoice.

Payments made by the County shall not preclude the right of the County from thereafter disputing any items or services involved or billed under this Contract and shall not be construed as acceptance of any part of the goods or services.
7. **Taxpayer ID Number:** The Contractor shall include its taxpayer ID number on all invoices submitted to the County for payment to ensure compliance with IRS requirements and to expedite payment processing.
8. **Payment – Invoicing Instructions:** The Contractor will provide an invoice on the Contractor's letterhead for goods delivered and/or services rendered. In the case of goods, the Contractor will leave an invoice with each delivery. Each invoice will have a number and will include the following information:

- a. Contractor's name and address

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

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

Invoice and support documentation are to be submitted to:

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

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

ATTACHMENT C**OCHCA SECURITY REQUIREMENTS AND GUIDELINES FOR CONTRACTORS AND
APPLICATION SERVICE PROVIDERS**

County of Orange Health Care Agency

**Security
Requirements and
Guidelines for
Application
Vendors and
Application Service
Providers**

04/2022

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 12 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. Passwords shall satisfy the following complexity rule:
 - Passwords will contain a minimum of one upper case letter
 - Passwords will contain a minimum of one lower case letter
 - Passwords will contain a minimum of one number: 1-0
 - Passwords will contain a minimum of one symbol: !, @, #, \$, %, ^, &, *, (,)
 - Password characters will not be sequential (Do not use: ABCD , This is ok: ACDB)
 - Passwords characters will not be repeated in a row (Do not use: P@\$\$S. This

is ok: P@\$\$)*COMPLEX PASSWORD EXAMPLE: P@\$SWoRd13

7 Audit Capabilities

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

8 Protection from Malicious Code

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

9 Remote Support Functionality

- Provider must conform to OCHCA Vendor Remote Access Policy.

10 HCA Data Usage

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

11 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:

- o **SSAE 18.** SSAE 18 SOC 2 Type 2 or SOC 3 compliance certificate
- o **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 agreement within their own organization as part of an overall security training and awareness program. At a minimum, vendor employees must sign a statement of understanding within their own organization regarding Internet dangers, IT security, and IT ethics and best practices,
- IT Security Policies and Procedures.
- **IT Operations Security Policy.** Written standards for operational security for any facilities where the County data, staff or systems shall exist. These documents must include, but not be limited to, physical security, network security, logical security, systems/platform security, wireless access, remote access, and data protections.
- **Data Management Security Policy.** Policy for the safeguarding and management of all data provided by the County or accessed by vendor as part of implementation and ongoing maintenance. This policy must, at a minimum, include check-in, check-out, copy control, audit logs and separation of duties.
- **Security Incident Notification and Management Process.** A detailed document that outlines the contact names and order and escalation of events that will occur in the case of a security breach concerning the County staff, data, or systems. This document must be updated immediately upon any

change. The vendor shall be held liable to the time-tables and protections outlined in the document.

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

- Bear the cost of compliance for any required changes to security infrastructure, policies and procedures to comply with existing regulations, unless such change is unique to the County.
- Comply with reasonable requests by the County for audits of security measures, including those related to identification and password administration.
- Comply with reasonable requests by the County for onsite physical inspections of the location from which the vendor provides services.
- Provide the County with any annual audit summaries and certifications, including but not limited to HIPAA, 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
- Security Contact Identification (24x7x365)
- Staff Related Items
 - Pre-Employment Screening Policy/Procedure
 - Background Checking Procedure
 - Ongoing Employment Status Validation Process
 - Staff Roster and Duties

ATTACHMENT E

GSA Contract No. GS-35F-0032U

**GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SCHEDULE PRICE LIST**

On-line access to contract ordering information, terms and conditions, up-to-date, pricing, and the option to create an electronic delivery order are available through GSA Advantage!®, a menu-driven database system. The INTERNET address GSA Advantage!® is: GSAAvantage.gov

MULTIPLE AWARD SCHEDULE

Large Category: INFORMATION TECHNOLOGY

Subcategory: IT Services

NOTE: Offerors are encouraged to identify within their software items any component interfaces that support open standard interoperability. An item's interface may be identified as interoperable on the basis of participation in a Government agency-sponsored program or in an independent organization program. Interfaces may be identified by reference to an interface registered in the component registry located at <http://www.core.gov>.

Contract Number: GS-35F-0032U

Period Covered by Contract: October 12, 2022 to October 11, 2027

Price list current through Modification PO-0065, effective August 1, 2022



Cority Software, Inc.
250 Bloor Street East
9th Floor, Box 15
Toronto, ON, Canada M4W 1E5
Phone Number: 416-863-6800
www.cority.com

Point of Contact for Contract Administration: Amanda Smith
Telephone: 734-277-6639
eMail: amanda.smith@cority.com

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at <http://fss.gsa.gov>

BUSINESS SIZE: OTHER THAN SMALL

CUSTOMER INFORMATION:

- 1a. Table of awarded Special Item Numbers:
511210 SOFTWARE PUBLISHER

- 1b. Identification of the lowest price model number for each SIN:

SIN	PRODUCT NAME	PRICE
511210	101: Medical Portal: 83,332 users or up	\$0.43

- 1c. Labor Category Descriptions and hourly rates: Not Applicable.
2. Maximum Order: \$500,000 for SIN 511210.
3. Minimum Order: \$100.
4. Geographic Coverage (delivery area): Domestic and overseas delivery.
5. Point(s) of production (city, county, and State or foreign country): Toronto, ON, Canada
6. Discount from list price or statement of net price: Prices shown herein are NET, basic discount has been deducted.
7. Quantity Discounts:
Dollar Volume:
\$150,000 to \$299,999 = an additional 2.5% discount
\$300,000 to \$499,999 = an additional 4.5% discount
\$500,000 = an additional discount to be negotiated on a case-by-case basis.
- *Please Note: Volume discounts in this area cannot be combined.
8. Prompt Payment Terms: None, Net 30 days.
9. Foreign Items (list items by country of origin): Canada
- 10a. Time of Delivery:
SIN 511210 7 Days After Receipt of Order (ARO)
- 10b. Expedited Delivery: Contact Cority Software, Inc.
- 10c. Overnight & 2-Day Delivery: Contact Cority Software, Inc.
- 10d. Urgent Requirements: Contact Cority Software, Inc.

CUSTOMER INFORMATION:

11. FOB Point(s): Destination
- 12a. Ordering Address:
Cority Software, Inc.
250 Bloor Street East
9th Floor, Box 15
Toronto, ON, Canada M4W 1E5
- 12b. Ordering Procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's) are found in Federal Acquisition Regulations (FAR) 8.405.3.
13. Payment Address:
Cority Software, Inc.
250 Bloor Street East
9th Floor, Box 15
Toronto, ON, Canada M4W 1E5
14. Warranty Provision: Standard Commercial Warranty.
15. Export packing charges, if applicable: Not Applicable.
16. Terms and conditions of rental, maintenance, and repair (if applicable): Not Applicable.
17. Terms and conditions of installation (if applicable): Not Applicable.
- 18a. Terms and conditions of repair parts indicating date of parts price list and any discounts from list prices (if applicable): Not Applicable.
- 18b. Terms and conditions for any other services (if applicable): Not Applicable.
19. List of service and distribution points (if applicable): Not Applicable.
20. List of participating dealers (if applicable): Not Applicable.
21. Preventative Maintenance (if applicable): Not Applicable.
- 22a. Special attributes such as environmental attributes (e.g., recycle content, energy efficiency, and/or reduced pollutants): Not Applicable.
- 22b. If applicable, indicate that Section 508 Compliance Information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor's website or other location). The EIT Standards can be found at: www.Section508.gov/.
23. Unique Entity Identifier (UEI): JKKKJ9PYWAP1
24. Notification regarding registration in System of Award Management (SAM) database: We are current in SAM.

Hosted Software & Service Agreement

1. Cority Software, Inc. will provide to the Client Cority Software, Inc.'s occupational health and safety software hosted by Cority Software, Inc. at its data centre and as specified in this Agreement. If requested by Client and specified on page 1 of this Agreement, the Reed Group MDG or ODG disability guidelines (the "Software"). The Client will contact Cority Software, Inc. if it requires additional modules or named user licenses. The Software will be Cority Software, Inc.'s standard application and will include updates and upgrades. For the purpose of this Agreement, updates mean changes or patches to be integrated with the Software to correct errors that do not alter the functionality or the content of the Software. Upgrades mean new versions, modifications or additions to the Software that alter the functionality or contents of the Software. Services for an upgrade project, such as training on the new version, will be provided as requested by the Client and as documented and at the rates specified in a Government Purchase Order. Any customizations requested by the Client will result in additional annual server and hosting fees as stated in the Government Purchase Order. If the Client wishes to apply the customizations to a future version of the Software, a separate Government Purchase Order shall be negotiated at that time.
2. Cority Software, Inc. will provide installation, Implementation and training services, as may be requested by the Client at Cority Software, Inc.'s daily or hourly rates, as specified in the Government Purchase Order.
3. Cority Software, Inc. will provide telephone support during the hours of 7 am to 7 pm EST Monday to Friday excluding federal holidays to the Client's end-users and technical support staff, including its duly authorized employees, agents, consultants and/or independent contractors ("employees," hereinafter). Prior to using Cority Software, Inc.'s telephone support services, the Client's end-users and employees are expected to have a reasonable familiarity with the Software either through formal training provided by Cority Software, Inc. or the equivalent in informal training provided by the Client's staff.

End-user telephone support is for the purpose of responding to possible errors in the Software or set-up of the Software and other issues of a technical nature. Telephone support does not include Implementation services, programming, report generation or resolution of the Client's computer system problems that are unrelated to the operation of the Software. Cority Software, Inc. will fully support the two most current versions of its Software and will support prior versions in accordance with its standard policies and procedures. Client may store up to 10 GB of data in its Cority Software, Inc.-hosted database. Client will pay for any data stored in excess of the 10 GB limit, as stated in the Government Purchase Order. The Annual Fee, as set out on the first page of this Agreement, will be invoiced quarterly in arrears. Cority Software, Inc. shall state separately on its invoices, taxes excluded from the fees, and the Government agrees to either pay the amount of the taxes (based on the current value of the equipment or services) to Cority Software, Inc. or provide it evidence necessary to sustain an exemption, in accordance with FAR 52.229-1 and FAR 52.229-3.

4. Fees for the implementation and training services will be invoiced monthly.
5. Cority Software, Inc.'s Software and its source code, object code, design, architecture, data base schema, and related documentation and information ("Cority Software, Inc. Confidential Information") are valuable intellectual property and the Client agrees (i) to protect and keep confidential the Cority Software, Inc. Confidential Information to the same degree that it protects its own confidential and proprietary information; (ii) not to transfer or provide the Cority Software, Inc. Confidential Information to third parties, on a service bureau basis or otherwise, or to disclose or make available the Cority Software, Inc. Confidential Information to third parties except agents, consultants, independent contractors or advisers who have a "need to know" and who are bound by similar non-disclosure obligations in favor of the Client; and (iii) not to duplicate, copy, reproduce, modify, transfer or distribute all or any part

of the Software except as consistent with the use of the Software as set out in this Agreement. Nothing contained herein shall prevent the Government from providing copies to its duly authorized employees. Cority Software, Inc. agrees that it

will protect and keep confidential, to the same degree that it protects its own confidential information, all information of a confidential nature received from the Client including, without limitation, protected health information, employee demographic information, and other information pertaining to Client's employees, processes, financials, and customers ("Client Confidential Information"). The obligations with respect to Cority Software, Inc. Confidential Information and Client Confidential Information shall continue indefinitely notwithstanding any termination of this Agreement. Neither party will acquire any right, title, or interest in the intellectual property rights owned by the other party by virtue of its performance under this Agreement. If any patentable or copyrightable ideas, writings, drawings, inventions, designs, parts, machines or processes developed as a result of, or in the course of, the work performed under this Agreement or under separately signed Government Purchase Orders for customizations by Cority Software, Inc. for the Client that cannot be separated from the Software ("Dependent Customizations"), Cority Software, Inc. shall own all right, title and interest in such Dependent Customizations. Cority Software, Inc. grants to Client a non-exclusive, perpetual, irrevocable, paid-up, royalty-free, nontransferable, world-wide license to use, make, have made, or copy such Dependent Customizations for the purposes contemplated in this Agreement. Notwithstanding anything to the contrary in this Agreement, Client shall own all right, title and interest, including copyrights and patent rights, in Changes that are unrelated to or reasonably severable in their functionality from the Software ("Stand-alone Customizations") and that are specified as Stand-alone Customizations in the customization documentation. The parties agree that such Stand-alone Customizations are "works made for hire," and Cority Software, Inc. hereby assigns all such rights, title and interest in such Stand-alone Customizations to Client and agrees to execute, upon Client's request, all papers necessary for vesting ownership in Client and obtaining formal legal protection for same in Client's name.

instrumentality of the US Government, recourse against the United States for any alleged breach of this Agreement must be made under the terms of the Federal Tort Claims Act or as a dispute under the contract disputes clause (Contract Disputes Act) as

6. This Agreement will be effective on the date signed by both parties. When the end user is an

applicable. During any dispute under the disputes clause, Cority Software, Inc. shall proceed diligently with performance of this contract, pending final resolution of any request for relief, claim, appeal, or action arising under the contract, and comply with any decision of the Contracting Officer. Cority Software, Inc. will issue a renewal notice a couple of months before the anniversary date to remind the Client to issue the Government Purchase Order for the subsequent year. In the event of the termination of this Agreement for any reason, Cority Software, Inc. will provide the Client with all of the Client's data in a textfile format and will fully cooperate with the Client in connection with such transfer of data.

7. Cority Software, Inc. agrees to defend and hold harmless the Client from and against any third party claim, suit, demand, action or proceeding arising from or relating to any breach by Cority Software, Inc. of its intellectual property rights to the Software. In the event that any suit, action, or other proceeding is asserted or brought against the Client alleging a violation of any intellectual property rights of a third party based upon the use of the Software, the Client will promptly notify Cority Software, Inc. and provide it with a copy of all relevant documentation. In the event the Software is held by a court, of competent jurisdiction to constitute an infringement or its use is enjoined, Cority Software, Inc. will, at its option, either: (i) work with the Government to procure its right to continue use of the Software; (ii) provide a modification to the Software so that its use becomes non-infringing; or (iii) replace the Software with software which is substantially similar in functionality and performance. Nothing contained herein shall operate in derogation of the U.S. Department of Justice's jurisdictional statute 28 U.S.C. § 516.
8. Cority Software, Inc. shall use all reasonable efforts to ensure that the software performs the functions as described in available product literature and specifications. Cority Software, Inc. does not make any warranties, express or implied, including the implied warranties of merchantability or fitness for any particular purpose other than for the stated purpose in the product material, to the Client. Neither party will be liable for any consequential,

special, indirect or exemplary damages or for

loss, damage, or expense directly or indirectly arising out of or in connection with the implementation or use of the Software either separately or in combination with any software, data communications or other equipment. Each party's liability for a breach of this Agreement shall in no event exceed two times the amount of fees paid under this Agreement except for any breaches of the intellectual property rights indemnification in Section 7 or the confidentiality obligations in Section 5 which are not subject to this limitation on liability. The foregoing exclusion/limitation of liability shall not apply (1) to personal injury or death caused by Cority Software, Inc.'s negligence; (2) for fraud; or (3) for any other matter for which liability cannot be excluded by law.

9. Cority Software, Inc. shall use managerial, operational, physical and technical safeguards and take such other actions as reasonably necessary, consistent with the practices and professional standards applied by first tier information technology service providers handling similarly sensitive information, to preserve and protect against any anticipated or actual threats or hazards to the integrity and security of, and prevent any unauthorized access to or destruction, use, modification and disclosure of, any data (including but not limited to name, address, telephone number, e-mail address, account number, Social Security number, regarding a Government employee and any other information that can be used to uniquely identify any Government employees ("Personally Identifiable Information") while in its possession and control hereunder. Such safeguards and actions shall include, without limitation: (a) development, implementation and maintenance of a comprehensive, written information security program; (b) proactive monitoring of known vulnerability points; (c) encryption of Personally Identifiable Information with industry standard encryption levels at all times while in transit or stored, including storage on portable equipment; (d) prohibition of personnel, including subcontractors and other third party service providers, from bringing transporting or transmitting Personally Identifiable Information to their homes, e-mail accounts or portable equipment; (e) adopting reasonable procedures in consultation with, or otherwise at

the request of, the Client for the safe, secure and accurate collection, processing, storage and transmission of Personally Identifiable Information, including but not limited to maintaining security settings and passwords as Confidential Information of Client, changing security settings and passwords with reasonable frequency and promptly installing updates, patches and security enhancements made available by vendors of any of the third party products used in connection with collection, processing, storage and transmission of Personally Identifiable Information; and (f) engagement of qualified, independent and reliable third parties to regularly audit and validate the data security measures maintained by Cority Software, Inc., in each case at Cority Software, Inc.'s own expense. Client reserves the right to review Cority Software, Inc.'s policies, procedures and practices used to maintain the privacy, security and confidentiality of Personally Identifiable Information. If Client discloses to Cority Software, Inc. or Cority Software, Inc. otherwise gains access to any Personally Identifiable Information in connection with this Agreement, Cority Software, Inc. may not use or disclose such Personally Identifiable Information for any purpose whatsoever, without Client's prior written consent, other than solely as necessary to provide the Services to Client and Authorized Users pursuant to this Agreement. In carrying out its activities under this Agreement, Cority Software, Inc. will observe and comply with all applicable data privacy and data protection laws and regulations, including Government privacy laws applicable to Cority Software, Inc.'s activities in connection with this Agreement. In addition, when accessing or handling any Personally Identifiable Information or other Client data, Cority Software, Inc. will comply with all written policies of Client that have been disclosed to Cority Software, Inc. in writing relating to the use and disclosure of such Personally Identifiable Information and other Client data. Cority Software, Inc. immediately shall notify Client if it becomes aware, or has reason to believe, that any breach of this Section has occurred, that any unauthorized access to or

use of, or any security breach relating to or otherwise affecting, any Personally Identifiable Information has occurred, or that any person who has had access to Personally Identifiable Information has violated or intends to violate the terms of this Agreement. Cority Software, Inc. shall, at its own expense, cooperate with Client in investigating and responding to the foregoing. Cority Software, Inc. shall be responsible for contractually requiring and causing any subcontractor or other third party service provider engaged by Cority Software, Inc. in connection with the Services to implement and comply with data security protections substantially similar to and no less protective than those provided in this Agreement.

10. None of the rights, duties and obligations of either party hereunder may be assigned, except in accordance with the provisions of the Anti-Assignment Act, 41 U.S.C. § 6305, and the procedures set forth in FAR 42.1204.
11. Any notices or other Communications required or permitted to be delivered hereunder shall be in writing and shall be delivered personally, by mail, by courier, or transmitted by facsimile to the parties at their respective addresses appearing on the execution page of this Agreement. Any notice, approval or communication so given shall be deemed received on the business day next following the date of delivery if in person or by facsimile, three days after delivery by courier and five days after delivery if by mail.
12. If circumstances beyond the control of the parties shall temporarily make it impossible for either or both of them to perform their Agreements hereunder, then the principles of force majeure shall apply and the right and obligations of the parties shall be temporarily suspended during the force

majeure period to the extent that such performance is reasonably affected.

13. Unless otherwise specifically provided herein, all amounts expressed or described hereunder are in U.S. currency.
14. This Agreement shall be governed and construed according to the laws of the United States and subject to the exclusive jurisdiction of the federal courts.



SIN 511210 Term Software Pricing

<u>SIN Number</u>	<u>Product Name</u>	<u>Product Description</u>	<u>No. of Users</u>	<u>Unit of Issue</u>	<u>GSA Price</u>
511210	100: Occupational Health Suite up to 9 users	Tracks medical trends, manage compliance and regulatory requirements, mitigate absences, and make informed decisions on how to improve employee health and productivity.	1 to 9 Users	Per User	\$2,569.27
	100: Occupational Health Suite:10-19 users		10 to 19 Users	Per User	\$2,389.42
	100: Occupational Health Suite:20-29 users		20 to 29 Users	Per User	\$2,055.42
	100: Occupational Health Suite:30-39 users		30 to 39 Users	Per User	\$1,926.95
	100: Occupational Health Suite:40-49 users		40 to 49 Users	Per User	\$1,413.10
	100: Occupational Health Suite:50-99 users		50 to 99 Users	Per User	\$1,156.17
	100: Occupational Health Suite:100-199 users		100 to 199 Users	Per User	\$899.24
	100: Occupational Health Suite:200 users and up		200 or More Users	Per User	\$642.32
511210	101: Medical Portal: 1 to 10,000 users	The Portal provides additional employees with streamlined access to the Cority Software, Inc. system.	1 to 10,000 Users	Per Group	\$8,563.23
	101: Medical Portal: 10,001 to 35000 users		10,001 to 35,000 Users	Per User	\$0.86
	101: Medical Portal: 35001 to 83331 users		35,001 to 83,331 Users	Per User	\$0.60
	101: Medical Portal: 83332 users and up		83,332 or More Users	Per User	\$0.43

SIN Number	Product Name	Product Description	No. of Users	Unit of Issue	GSA Price
511210	102: Electronic Prescription: 1-5 users	Prescribes medications (non-controlled substance medication only) for employees electronically, view ePrescription statuses and refill requests, Manage refill requests electronically by choosing to approve or deny the request, or to	1 to 5 Users	Per User	\$411.08
		prescribe a different medication instead, and view and monitor ePrescription interaction notifications and transaction log messages.			
	102: Electronic Prescription: 6 users and up		6 or More Users	Per User	\$154.16
511210	103: EPCS	Electronic Prescription Controlled Substances - Prescribes medications containing controlled substances for employees electronically, view ePrescription statuses and refill requests, Manage refill requests electronically by choosing to approve or deny the request, or to prescribe a different medication instead, and view and monitor ePrescription interaction notifications and transaction log messages.	1 or More Users	Per User	\$513.85
511210	300: Industrial Hygiene Suite: 1 to 9 users	Enables industrial hygienists to effectively identify hazards and mitigate risks to promote a healthy work environment.	1 to 9 Users	Per User	\$2,997.48
	300: Industrial Hygiene Suite: 10 to 19 users		10 to 19 Users	Per User	\$2,697.73
	300: Industrial Hygiene Suite: 20 to 29 users		20 to 29 Users	Per User	\$2,397.98
	300: Industrial Hygiene Suite: 30 to 39 users		30 to 39 Users	Per User	\$2,248.11
	300: Industrial Hygiene Suite: 40 to 49 users		40 to 49 Users	Per User	\$1,648.61
	300: Industrial Hygiene Suite: 50 to 99 users		50 to 99 Users	Per User	\$1,348.87
	300: Industrial Hygiene Suite: 100 users and up		100 or More Users	Per User	\$1,049.12

SIN Number	Product Name	Product Description	No. of Users	Unit of Issue	GSA Price
511210	350: Bayesian Decision Analysis	Bayesian decision analysis (BDA) is a form of statistical analysis of occupational exposure data that allows hygienists to select the most appropriate exposure category, even with limited data. BDA results in easy to interpret "decision charts", permits the user to mathematically incorporate prior information and professional judgment into the analysis, and can handle non-detects. It can also be used to select the most appropriate level of respiratory protection for those difficult to control exposure scenarios.	1 or More Users	Per User	\$256.93
511210	400: Safety Suite: 1 to 9 users	Enables organizations to efficiently manage safety risks and compliance items and streamline safety programs	1 to 9 Users	Per User	\$4,282.12
	400: Safety Suite: 10 to 19 users		10 to 19 Users	Per User	\$3,211.59
	400: Safety Suite: 20 to 29 users		20 to 29 Users	Per User	\$2,783.38
	400: Safety Suite: 30 to 39 users		30 to 39 Users	Per User	\$1,926.95
	400: Safety Suite: 40 to 49 users		40 to 49 Users	Per User	\$1,498.74
	400: Safety Suite: 50 to 99 users		50 to 99 Users	Per User	\$856.42
	400: Safety Suite: 100 users and up		100 or More Users	Per User	\$428.21
511210	402: Safety Portal Users: 1 to 10000 users	The Portal provides additional employees with streamlined access to the Cority Software, Inc. system.	1 to 10,000 Users	Per Group	\$8,563.23
	402: Safety Portal Users: 10001 to 35000 users		10,001 to 35,000 Users	Per User	\$0.86
	402: Safety Portal Users: 35001 to 83331 users		35,000 to 83,331 Users	Per User	\$0.60
	402: Safety Portal Users: 83332 users and up		83,332 Users or More	Per User	\$0.43

SIN Number	Product Name	Product Description	No. of Users	Unit of Issue	GSA Price
511210	500: Training Management Suite: 1 to 9 users	Provides EHS professionals with the ability to easily manage course details and participation activity for general safety training as well as training courses required for various surveillance programs.	1 – 9 Users	Per User	\$1,027.71
	500: Training Management Suite: 10 to 19 users		10 – 19 Users	Per User	\$924.94
	500: Training Management Suite: 20 to 29 users		20 – 29 Users	Per User	\$873.55
	500: Training Management Suite: 30 to 49 users		20 – 49 Users	Per User	\$822.17
	500: Training Management Suite: 50 to 99 users		50 – 99 Users	Per User	\$770.78
	500: Training Management Suite: 100 users and up		100 and Up Users	Per User	\$719.40
511210	600: Ergonomics Suite: 1 to 9 users	Empowers ergonomists with a complete solution for effectively managing ergonomics data collection and assessments.	1 to 9 Users	Per User	\$2,141.06
	600: Ergonomics Suite: 10 to 19 users		10 to 19 Users	Per User	\$1,819.90
	600: Ergonomics Suite: 20 to 29 users		20 to 29 Users	Per User	\$1,712.85
	600: Ergonomics Suite: 30 to 49 users		30 to 49 Users	Per User	\$1,605.79
	600: Ergonomics Suite: 50 to 99 users		50 to 99 Users	Per User	\$1,498.74
	600: Ergonomics Suite: 100 users and up		100 or More Users	Per User	\$1,070.53

SIN Number	Product Name	Product Description	No. of Users	Unit of Issue	GSA Price
511210	700: Environmental Suite: 1 to 9 users	Helps companies centralize and streamline the tracking and collection of key corporate environmental health and safety data and satisfy Environmental Management Systems (EMS) requirements.	1 to 9 Users	Per User	\$2,140.06
	700: Environmental Suite: 10 to 19 users		10 to 19 Users	Per User	\$2,034.01
	700: Environmental Suite: 20 to 29 users		20 to 29 Users	Per User	\$1,819.90
	700: Environmental Suite: 30 to 49 users		30 to 49 Users	Per User	\$1,712.85
	700: Environmental Suite: 50 to 99 users		50 to 99 Users	Per User	\$1,498.74
	700: Environmental Suite: 100 users and up		100 or More Users	Per User	\$1,070.53
Ancillary Offerings:					
511210	ODG Guidelines - Web Version 1 user	Official Disabilities Guideline Book web version.	1 User	Per User	\$513.00
	ODG Guidelines - Web Version 2 to 5 users		2 to 5 Users	Per User	\$471.03
	ODG Guidelines - Web Version 6 to 9 users		6 to 9 Users	Per User	\$449.62
	ODG Guidelines - Web Version 10 to 24 users		10 to 24 Users	Per User	\$406.80
	ODG Guidelines - Web Version 25 to 49 users		25 to 49 Users	Per User	\$385.39
	ODG Guidelines - Web Version 50 to 99 users		50 to 99 Users	Per User	\$363.98
	ODG Guidelines - Web Version 100 to 200 users		100 to 200 Users	Per User	\$321.16
	ODG Guidelines - Web Version 201 to 9998 users		201 to 9,998 Users	Per User	\$299.75
	ODG Guidelines - Web Version 9999 users and up		9,999 or More Users	Per User	\$256.93

SIN Number	Product Name	Product Description	No. of Users	Unit of Issue	GSA Price
Ancillary Offerings (Cont'd.):					
511210	30B MD Guidelines w/ Treatment (Annual Fee) - 1 to 15 users	Clinical disability durations and return to work guidelines for physicians, employers, case managers, and patients with treatment options.	1 to 15 Users	Per User	\$636.88
	30B MD Guidelines w/ Treatment (Annual Fee) - 16 to 49 users		16 to 49 Users	Per User	\$526.29
	30B MD Guidelines w/ Treatment (Annual Fee) - 50 to 100 users		50 to 100 Users	Per User	\$485.80
	30B MD Guidelines w/ Treatment (Annual Fee) - 101 to 200 users		101 to 200 Users	Per User	\$447.29
	30B MD Guidelines w/ Treatment (Annual Fee) - 201 to 300 users		201 to 300 Users	Per User	\$413.72
	30B MD Guidelines w/ Treatment (Annual Fee) - 301 users and up		More than 300 Users	Per User	\$382.13
511210	Installation and Implementation Services	Installation and Implementation Services	Per Hour	Per Hour	\$217.23
511210	Admin User	Administrative User Fee	Per user	Per User	\$2,569.27

SIN Number	Product Name	Product Description	No. of Users	Unit of Issue	GSA Price
Ancillary Offerings (Cont'd.):					
511210	One Time ASP Setup Fee	One Time ASP Setup Fee	Per Order	Per Order	\$9,874.06
511210	Data Storage	Per month fee for each GB of storage required by the customer above the free first 10GB/Month.	Per GB /Month	Per GB/Month	\$9.87