ADOPTED
BOARD OF SUPERVISORS
COUNTY OF LOS ANGELES
58 September 12, 2023
CELIA ZAVALA
EXECUTIVE OFFICER

Health Services
LOS ANGELES COUNTY

313 N. Figueroa Street, Suite 912
Los Angeles, CA 90012

Tel: (213) 288-8050
Fax: (213) 481-0503

www.dhs.lacounty.gov

"To advance the health of our patients and our communities by providing extraordinary care"

www.dhs.lacounty.gov

September 12, 2023

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, California 90012

Dear Supervisors:

APPROVAL OF AMENDMENT NO. 12 TO SOLE SOURCE AGREEMENT NO. H-212780 WITH ESO SOLUTIONS, INC. FOR AN UPGRADED TRAUMA AND EMERGENCY MEDICINE INFORMATION SYSTEM (ALL SUPERVISORIAL DISTRICTS) (3 VOTES)

CIO RECOMMENDATION: APPROVE (X) APPROVE WITH MODIFICATION ( ) DISAPPROVE ( )

SUBJECT

Request approval of Amendment No. 12 to the existing Sole Source Agreement No. H-212780 (Agreement) with ESO Solutions, Inc. (ESO) to upgrade one of the four data registries of the Trauma and Emergency Medicine Information System (TEMIS), LA Fire Rescue, to the Emergency Medical Services (EMS) Repository, a Software-as-a-Service (SaaS) platform; extend the term for use of the TEMIS; increase the contract sum; amend the Statement of Work (SOW); and update the Agreement's terms and conditions for the Department of Health Services (DHS), EMS Agency.

IT IS RECOMMENDED THAT THE BOARD:

1. Authorize the Director of Health Services (Director), or designee, to execute Amendment No. 12 to Sole Source Agreement No. H 212780 with ESO to: (a) extend the Agreement's term from October 1, 2023 through September 30, 2026 to ensure the necessary upgrade and continuation of

maintenance services of the TEMIS; (b) increase the maximum contract sum for the extension term by $6,037,507 from $18,766,888 to $24,804,395 which includes fifteen percent above the maximum Contract Sum of the three-year extension term in the amount of $787,501 in pool dollars to fund additional work.

2. Approve the annual budget allocation of Measure B Special Tax Fund to cover the cost of the Agreement with ESO for the upgrade, maintenance, and support of the DHS EMS Agency's TEMIS with a cost of $2,593,405 for October 1, 2023 through September 2024, $1,692,726 for October 1, 2024 through September 2025, and $1,751,376 for October 1, 2025 through September 2026.

3. Delegate authority to the Director, or designee, to execute future amendments to the Agreement to: a) use pool dollars to fund additional work, (b) incorporate administrative changes to the Agreement, including but not limited to: addition, modification, or removal of any relevant terms and conditions as required under Federal or State law or regulation, Los Angeles County (LA County) policy, Board of Supervisors (Board) and/or Chief Executive Office (CEO); and (c) approve necessary changes and modifications to the Statement of Work (SOW), with all actions subject to review and approval by County Counsel.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

Background

The current TEMIS Agreement with ESO expires on September 30, 2023. An amendment is needed to allow for its continued use by LA County. TEMIS is an integrated Countywide Trauma and Emergency Data Management System used by the EMS Agency, 15 trauma centers, 21 paramedic base hospitals and 32 EMS provider agencies. The EMS content and format of the existing TEMIS has been designed and customized for all of the agencies to continually access TEMIS records to generate reports necessary for timely data capture, analysis, and sharing of health intelligence data. The current TEMIS contains over 20 million records with more than 850,000 new records added annually.

TEMIS consists of four data registries: LA Fire Rescue, LA Base, LA Trauma, and TEMIS Central. Aside from providing for LA County's continued use of TEMIS, this Amendment also covers the upgrade of the legacy client-based LA Fire Rescue to the EMS Repository, which is a software platform hosted by the contractor, in the cloud, and accessible over the Internet as a SaaS solution to gather real-time EMS incident and patient level data.

The EMS Agency requires a software platform that is SaaS to gather real-time emergency medical services incident and patient level data, continue to provide LA County with the technology required to ensure timely data capture, analysis and sharing of health intelligence data, enhanced bio-surveillance, expedited decision-making for casualty management activities, and related hospital data to analyze health information necessary for emergency medical services system management and to meet LA County, State, and Federal reporting requirements for the EMS Agency.

Recommendations

Approval of the first recommendation will allow the Director, or designee, to execute Amendment No. 12 to Agreement No. H-212780, substantially similar to Exhibit I, to extend the term of the Agreement through September 30, 2026. Also, ESO will provide LA County with a cloud-based and fully hosted system, to be referred to as "EMS Repository NEMSIS 3.5 Standard" (EMS Repository). This will upgrade the client-based legacy LA Fire Rescue data registry, which is one of the four aforementioned data registries of EMS's TEMIS that is utilized to collect patient level information and patient care provided by EMS provider agencies (fire departments and ambulance operators) to patients in the pre-hospital setting. The other three databases (LA Base, LA Trauma and TEMIS Central) collect patient-level information from base hospitals and trauma centers.

TEMIS Central is a database that combines all three databases (LA Fire Rescue, LA Base, and LA Trauma) in order to have one record per patient thereby demonstrating the continuity of care rendered by EMS providers, base hospitals and trauma centers to each "9-1-1" patient. Also, TEMIS is utilized to analyze health information necessary for EMS system management and to meet LA County, State and Federal reporting requirements. TEMIS information is also utilized to share significant information between EMS provider agencies, "9-1-1" receiving facilities, and LA County.

Further, ESO will continue to provide and support the other three databases (LA Base, LA Trauma, and TEMIS Central) until they are fully transitioned to the SaaS platform. Also, the EMS Repository will be compliant and certified with the most current National Emergency Medical Services Information System (NEMSIS) standards and specifications.

ESO has established a history of responding consistently and quickly to the changing needs and demands of the EMS Agency, trauma centers, paramedic base hospitals and EMS provider agencies. ESO personnel have a comprehensive understanding of LA County's EMS system and have established and maintained an excellent working relationship with the existing TEMIS participants.

Approval of the second recommendation will allow the Director, or designee, to approve the annual budget allocation of Measure B Special Tax Fund to cover the cost of the Agreement with ESO for the upgrade, maintenance, and support of the DHS EMS Agency's TEMIS with a cost of $2,593,405 for October 1, 2023 through September 2024, $1,692,726 for October 1, 2024 through September 2025, and $1,751,376 for October 1, 2025 through September 2026.

Approval of the third recommendation will allow the Director, or designee, to execute future amendments to the Agreement to incorporate administrative changes to the Agreement, including but not limited to: addition, modification, or removal of any relevant terms and conditions as required under Federal or State law or regulation, LA County policy, Board and/or CEO, approve necessary changes to the SOW, and to use pool dollars for the ongoing and continuation of services, to acquire additional components for TEMIS, and for additional work during the extension term, as requested by LA County, with all actions subject to review and approval by County Counsel.

Implementation of Strategic Plan Goals

The recommended actions support Goal III. "Realize Tomorrow's Government Today, Strategy III.2.1 Enhance Information Technology Platforms to Securely Share and Exchange Data of LA County's Strategic Plan and Goals."

FISCAL IMPACT/FINANCING

The maximum contract sum under the Agreement will increase by $6,037,507 for the period of October 1, 2023 through September 30, 2026, which will be fully funded through the Measure B Special Tax Fund, the LA County's Trauma, Emergency and Bioterrorism Response Tax.

Funding request of $1,945,054 for Fiscal Year (FY) 2023-24 has been included in DHS FY 2023-24's Supplemental Budget Resolution request pending Board approval on October 3, 2023. DHS will request funding in future fiscal years, as needed. There is no impact to net County cost.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The Agreement, as amended by the recommended Amendment No. 12, includes all Board required provisions. The Agreement may be terminated for convenience by LA County upon a 30-day prior written notice.

County Counsel has approved Exhibit I as to form. In compliance with Board Policy 6.020 "Chief Information Office Board Letter Approval", the Office of the Chief Information Officer (OCIO) reviewed the Information Technology (IT) components of this request and recommends approval. The OCIO concurs with the Department's recommendation and that office's analysis is attached (Attachment A).

The Department has determined that the TEMIS services provided by ESO are highly specialized and cannot be provided by LA County staff, and therefore, not subject to the Living Wage Program (LA County Code Chapter 2.201).

The EMS Agency will use Measure B funds to cover the annual cost of the Agreement for the maintenance and support of the legacy TEMIS data repositories during the upgrade of TEMIS to a SaaS application software. Both the EMS Agency and system users, including public and private acute care hospitals with an emergency department and EMS providers, access records in TEMIS to generate reports necessary for daily operations such as contract monitoring, system audits, and performance improvement activities.

Measure B is a ballot initiative that was passed by the voters of LA County on November 6, 2002, and provides funding for trauma and emergency services as well as bioterrorism preparedness. Also, Measure B allows for the expenditure of funds to maintain and expand the trauma network LA Countywide, while ensuring more timely and effective responses to critical and urgent medical emergencies, and biological and chemical terrorism threats.

CONTRACTING PROCESS

The Amendment is being recommended to extend the contractual relationship with ESO on a sole source basis.

On January 24, 2022, DHS notified the Board of its intent to enter into sole source negotiations for the extension of the Agreement with ESO in accordance with Board Policy No. 5.100 (Attachment B).

The sole source checklist (Attachment C) is attached in compliance with this policy.

State regulations require local EMS agencies to submit EMS records to the State and federal EMS data registries that are compliant with NEMSIS standards. The upgrade of the EMS Repository is necessary for the EMS Agency to comply with State regulations on data collection and reporting requirements.

Also, it is in the best economic interest of LA County (and the trauma centers, base hospitals and EMS provider agencies) to extend the Agreement term given the significant costs to replace the existing system and infrastructure, as well as the administrative burden that the entire trauma system would experience via an excessive learning curve to implement a replacement system.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Approval to execute Amendment No. 12 will not infringe on the role of LA County in its relationship to its residents, and LA County's ability to respond to emergencies will not be impaired. Also, the Agreement will not result in reduced services, and there is no employee impact as a result of this Agreement since services are currently being provided under an Agreement.

Approval of the recommendations will ensure EMS Agency continues to provide uninterrupted critical patient care needs while a portion of TEMIS is upgraded to a SaaS platform for the timely data capture, analysis and sharing of health intelligence data and to comply with LA County, State and Federal reporting requirements.

Respectfully submitted,

Christina R. Ghaly, M.D.
Director

Peter Loo
Acting Chief Information Officer

CRG:az

Enclosures

c: Chief Executive Office
County Counsel
Executive Office, Board of Supervisors

Chief Information Office

Peter Loo
ACTING CHIEF INFORMATION OFFICER

CIO ANALYSIS

BOARD AGENDA DATE:
9/12/2023

SUBJECT:

APPROVAL OF AMENDMENT NO. 12 TO SOLE SOURCE AGREEMENT NO. H-212780 WITH ESO SOLUTIONS, INC. FOR AN UPGRADED TRAUMA AND EMERGENCY MEDICINE INFORMATION SYSTEM

CONTRACT TYPE:

☐ New Contract ☐ Sole Source ☒ Amendment to Contract #: H-212780

SUMMARY:

Description:

The Department of Health Services (DHS) is requesting approval of Amendment No. 12 to the existing Agreement with ESO Solutions, Inc. to upgrade one of the four data registries of the Trauma and Emergency Medicine Information System (TEMIS) to a Software-as-a-Service (SaaS) platform, extend the term for use of TEMIS for three years (from Oct. 1, 2023 through Sept. 30, 2026) and increase the Contract Sum by $6,037,507, including $787,501 in Pool Dollars for additional, as needed, work. This Amendment will increase the maximum Contract sum from $18,766,888 to $24,804,395.

DHS is also requesting approval of the annual budget allocation of Measure B Speical Tax Fund to cover the cost of this Amendment.

Additionally, DHS is requesting delegated authority to the Director, or designee, to execute future amendments to the Agreement to use Pool Dollars to fund additional work, incorporate administrative changes to the Agreement and approve necessary changes and modifications to the Statement of Work, with all actions subject to review and approval by County Counsel.

Under this proposed Amendment, ESO Solutions will extend the Agreement by three years, and provide the County with a Software-as-a-Service fully hosted system for the legacy LA Fire-Rescue data registry, which is one of four data registries supported by TEMIS, and used to collect patient level information and patient care provided by EMS provider agencies (fire departments and ambulance operators).

Contract Amount: $6,037,507 for this Amendment

APPROVAL **OF AMENDMENT NO. 12 TO SOLE SOURCE AGREEMENT NO. H-212780 WITH ESO SOLUTIONS, INC. FOR AN UPGRADED TRAUMA AND EMERGENCY MEDICINE INFORMATION SYSTEM**

FINANCIAL ANALYSIS:

Contract costs:

Three-year costs

Regisgtry Replatforming and SaaS fees.....	$	5,250,006
Contract Pool Dollars	$	787,501
Total costs:	**$**	**6,037,507**

Notes:

This Amendment will be fully funded through Measure B Special Tax Fund (County's Trauma, emergency and Bioterrorism Response Tax). Measure B is a ballot initiative that was passed by the voters of Los Angeles County on November 6, 2002, and provides funding for trauma and emergency services as well as bioterrorism preparedness. Also, Measure B allows for the expenditure of funds to maintain and expand the trauma network Countywide, while ensuring more timely and effective responses to critical and urgent medical emergencies, and biological and chemical terrorism threats.

Funding request of $1,945,054 for Fiscal Year (FY) 2023-24 has been included in DHS FY 2023-24 Supplemental Budget request. DHS will request funding in future fiscal years, as needed.

This Amendment will increase the Maximum Contract Sum from $18,766,888 to $24,804,395.

RISKS:

1. **Quality of Services:** The Amendment includes a Service Level Agreement of 99.5% uptime. If the the 99.5% uptime metric is not met for any calendar month, the County shall receive a credit equal to 10% of the annual fee. Other key components included in the Amendment include: Functional, Technical and Hosting requirements, Data Conversion, Business Continuity and Disaster Recovery, Support and Maintenance Services and Implementation Plan. The Statement of Work is well-structured and includes the Major Tasks, each with a defined set of Deliverables. The seven Major Tasks include:
    - Project Administration
    - Build and Implement the EMS Repository on SaaS
    - Conduct Acceptance Teste for the EMS Repository
    - Maintain legacy data from LA Fire-Rescue data registry
    - Training
    - Deployment to production
    - Post Go-live support
2. **Project Management and Governance:** To ensure project success, the Office of the Chief Information Officer (OCIO) recommends strong project governance and a dedicated project manager to adhere to schedule, budget and scope, and to manage vendor performance. Because this project only includes the replatforming of one of the four system registries, DHS will not use a Project Steering Committee. However, the project has an Executive Sponsor and a Dedicated Project Manager.
3. **Information Security:** The County's Office of the Chief Information Security Officer (OCISO) reviewed the Amendment with the DHS Department Information Security Officer (DISO) and assessed the project as low risk. Being a SaaS solution, the SOC II report (independent third-party assessment on security controls) was reviewed, including the vendor-completed County SaaS Security Questionnaire with no concerns or issues. The system and data are logically segregated to address confidentiality. The contract also includes Cyber Liability Insurance with limits of $8,000,000 per occurrence and in the aggregate.
4. **Contract Risks:** No contract risks have been identified. County Counsel participated in the negotiation and approved the Amendment as to form. The contract includes:
    - Limitation of Liability of $9 Million.
    - County's standard requirements for Commercial General Liability Insurance.

APPROVAL **OF AMENDMENT NO. 12 TO SOLE SOURCE AGREEMENT NO. H-212780 WITH ESO SOLUTIONS, INC. FOR AN UPGRADED TRAUMA AND EMERGENCY MEDICINE INFORMATION SYSTEM**

PREPARED BY:

Henry Belta — 7/27/2023

(NAME) DEPUTY CHIEF INFORMATION OFFICER — DATE

APPROVED:

Peter Loo — 8/2/2023

PETER LOO, ACTING CHIEF INFORMATION OFFICER — DATE

Attachment B

Health Services
LOS ANGELES COUNTY

January 24, 2022

313 N. Figueroa Street, Suite 912
Los Angeles, CA 90012

Tel: (213) 288-8050
Fax: (213) 481-0503

www.dhs.lacounty.gov

"To advance the health of our patients and our communities by providing extraordinary care"

TO: Supervisor Holly J. Mitchell, Chair
Supervisor Hilda L. Solis
Supervisor Sheila Kuehl
Supervisor Janice Hahn
Supervisor Kathryn Barger

FROM: Christina R. Ghaly, M.D.
Director

SUBJECT: **ADVANCE NOTIFICATION OF INTENT TO EXTEND SOLE SOURCE AGREEMENT NO. H-212780 WITH ESO SOLUTIONS, INC.**

This is to advise the Board of Supervisors (Board) that the Department of Health Services (DHS or Department) intends to request approval of an extension to the existing sole source agreement with ESO Solutions, Inc. (ESO) for the Trauma and Emergency Medicine Information System (TEMIS) Application Software and Support Services, Agreement No. H-212780 (Agreement), used by the DHS Emergency Medical Services (EMS) Agency, 15 trauma centers, 21 base hospitals and 39 EMS provider agencies (collectively the Los Angeles County (LA County) EMS System). DHS has determined that continuity of this Agreement is essential to LA County's compliance with State and federal data collection requirements, and in the best economic interest of LA County to extend the Agreement term.

Board Policy No. 5.100 requires written notice of a department's intent to enter into sole source negotiations for an extension of a Board-approved agreement at least six months prior to the agreement's expiration date. DHS will exhaust its delegation of authority to extend the Agreement on June 30, 2022.

Background

The EMS Agency serves as the lead agency for the emergency medical services system in LA County and is responsible for coordinating all system participants within its jurisdiction, encompassing both public and private sectors. LA County's EMS Agency has one of the largest EMS systems in the nation and, as one of the first to be developed, is known nationally and worldwide as a leader in the field of pre-hospital care. The system utilizes over 18,000

certified EMS personnel employed by fire departments, law enforcement, ambulance companies, hospitals and private organizations to provide lifesaving care to those in need 24 hours a day, seven days a week.

LA County and Lancet Technology, Inc. (Lancet) entered into the Agreement for TEMIS Application Software and Support Services on June 19, 2001. This Agreement was subsequently assigned and delegated to ESO Trauma Holdings, LLC (a wholly-owned subsidiary of ESO).

TEMIS is an integrated, Countywide trauma and emergency clinical data management system developed by Lancet and used by the entities that make up the LA County EMS System, all of whom rely on TEMIS for access to data and to generate reports necessary for timely data capture, analysis, and health intelligence data sharing. TEMIS provides a single patient record information system throughout the entire continuum of emergency care. Every 9-1-1 call is collected and tracked in TEMIS starting with the EMS provider (jurisdictional fire district and 9-1-1 responding ambulance company), continuing through the receiving base hospital or trauma center until patient discharge, and patient records from TEMIS are matched based on unique identifiers using an automated nightly process. TEMIS is used to meet Federal National Trauma Data Bank and State of California EMS Information System data collection requirements. Also, TEMIS is funded and fully offset by Measure B (Special Tax Revenue Fund) and base hospital fees.

The Agreement has been amended several times to upgrade the TEMIS application software, increase the Contract Sum to $17,373,542 and extend the Agreement term to June 30, 2022. The most recent amendment was executed due to ESO receiving a significant strategic investment from Vista Equity Partners (Vista) making Vista the majority controlling shareholder of ESO. However, ESO's corporate existence, management and employees remained the same, and ESO remains the active operating company for this Agreement.

Justification

TEMIS is a proprietary product developed and customized for LA County and owned by ESO. TEMIS has evolved from its original form into a more complex and customized system that allows for enhanced bio-surveillance and expedited decision making for casualty management activities. ESO has a comprehensive understanding of LA County's EMS system and has established an excellent working relationship with the existing TEMIS participants. Also, ESO has established a positive track-record of responding consistently and quickly to all of the demands of the system's participants.

As mentioned above, TEMIS is necessary to meet Federal National Trauma Data Bank and State of California EMS Information System data collection requirements. Through the Agreement with ESO, LA County (via TEMIS) has amassed approximately 20 years' worth of patient record information that would have to be migrated into a new system. It

is also in the best economic interest of LA County (and the trauma centers, base hospitals and EMS provider agencies) to extend the Agreement term given the significant costs to replace the existing system and infrastructure, as well as the administrative burden to the entire trauma system would experience via an excessive learning curve to implement a replacement system.

DHS intends to negotiate an extension to continue the services while evaluating the best course of action to ensure that the future needs of LA County EMS System are met.

If this Agreement is not extended, DHS will lose access to all existing customized EMS content and data developed by one of the largest EMS organizations in the nation. TEMIS has been designed and customized for all the agencies in the LA County EMS System to continually access TEMIS records in order to generate reports necessary for timely data capture, analysis and sharing of health intelligence data. Also, TEMIS contains more than 12 million records, with more than 850,000 new records added annually.

Conclusion

DHS has determined that ESO is uniquely positioned to continue providing the trauma and emergency clinical data management system and services that will permit DHS facilities to continue meeting their EMS needs without interruption. DHS will commence negotiations for the Agreement's extension no earlier than four weeks from the date of this notification unless otherwise instructed by the Board.

If you have any questions, you may contact me or your staff may contact Richard Tadeo, Emergency Medical Services Assistant Director at (562) 378-1610 or by email at rtadeo@dhs.lacounty.gov.

CRG:as

c: Chief Executive Office
County Counsel
Executive Office, Board of Supervisors
Chief Information Office

ATTACHMENT C

SOLE SOURCE CHECKLIST

Department Name: _____

☐ New Sole Source Contract

☐ Sole Source Amendment to Existing Contract
Date Existing Contract First Approved: _____

Check (✓)	**JUSTIFICATION FOR SOLE SOURCE CONTRACTS** **Identify applicable justification and provide documentation for each checked item.**
	➢ Only one bona fide source (monopoly) for the service exists; performance and price competition are not available. A monopoly is an "*Exclusive control of the supply of any service in a given market. If more than one source in a given market exists, a monopoly does not exist* ."
	➢ Compliance with applicable statutory and/or regulatory provisions.
	➢ Compliance with State and/or federal programmatic requirements.
	➢ Services provided by other public or County-related entities.
	➢ Services are needed to address an emergent or related time-sensitive need.
	➢ The service provider(s) is required under the provisions of a grant or regulatory requirement.
	➢ Additional services are needed to complete an ongoing task and it would be prohibitively costly in time and money to seek a new service provider.
	➢ Services are needed during the time period required to complete a solicitation for replacement services; provided services are needed for no more than 12 months from the expiration of an existing contract which has no available option periods.
	➢ Maintenance and support services are needed for an existing solution/system during the time to complete a solicitation for a new replacement solution/ system; provided the services are needed for no more than 24 months from the expiration of an existing maintenance and support contract which has no available option periods.
	➢ Maintenance service agreements exist on equipment which must be serviced by the original equipment manufacturer or an authorized service representative.
	➢ It is more cost-effective to obtain services by exercising an option under an existing contract.
	➢ It is in the best economic interest of the County (e.g., significant costs to replace an existing system or infrastructure, administrative cost savings and excessive learning curve for a new service provider, etc.) In such cases, departments must demonstrate due diligence in qualifying the cost-savings or cost-avoidance associated with the best economic interest of the County.

Erika Bonilla
_____
Chief Executive Office

_____
Date

EXHIBIT I

AMENDMENT NUMBER TWELVE TO

COUNTY AGREEMENT NUMBER H-212780

BY AND BETWEEN

COUNTY OF LOS ANGELES

AND

ESO SOLUTIONS, INC.

FOR

TRAUMA AND EMERGENCY MEDICINE INFORMATION SYSTEM (TEMIS)

APPLICATION SOFTWARE AND SUPPORT SERVICES

September 2023

AMENDMENT NUMBER TWELVE

TO

AGREEMENT BY AND BETWEEN

THE COUNTY OF LOS ANGELES AND ESO SOLUTIONS, INC.

FOR

TRAUMA AND EMERGENCY MEDICINE INFORMATION SYSTEM (TEMIS)

APPLICATION SOFTWARE AND SUPPORT SERVICES

This AMENDMENT is made and entered into this _____ day of September 2023 (hereinafter "Amendment No. 12 Date"),

By and between — COUNTY OF LOS ANGELES (hereinafter "County")

And — ESO SOLUTIONS, INC.
Business Address:
11500 Alterra Parkway, Suite 100
Austin, TX 78758
(hereinafter "Contractor")

WHEREAS, reference is made to that certain Agreement No. H-212780 for Trauma and Emergency Medicine Information System (TEMIS) Application Software and Support Services, dated June 19, 2001, including any amendments and other modifications thereto (hereinafter cumulatively "Agreement"); and

WHEREAS, the parties have executed Amendment Nos. One through Ten throughout the term of the Agreement; and

WHEREAS, on September __, 2023, the Board of Supervisors (Board) delegated authority to the Director of Health Services, or authorized designee, to, among other delegations, (i) extend the term of the Agreement, (ii) increase the Contract Sum, (iii) incorporate administrative changes to the Agreement, including but not limited to, addition, modification, or removal of any relevant terms and conditions and to comply with changes in applicable law, (iv) approve necessary changes to the Statement of Work (SOW), and (v) execute future Amendments and/or Change Notices using Pool Dollars to acquire Additional Work described in the Agreement as needed, subject to the review and approval by County Counsel, and, if applicable, the Office of the Chief Information Office; and

WHEREAS, the Agreement is slated to expire on September 30, 2023; and

WHEREAS, it is the intent of the parties hereto to continue to allow the County to use the TEMIS and to upgrade one of the four data repositories, the EMS Repository, to a software platform hosted by the Contractor in the cloud and accessible over the Internet via a website (commonly referred to as software-as-a-service (SaaS)) to gather real-time EMS incident and patient level data, and as such, this Amendment No. Twelve will: (i) amend the Agreement to extend its term from

October 1, 2023 through September 30, 2026, to continue to provide County with the TEMIS technology required to ensure timely data capture, analysis and sharing of health intelligence data, enhanced bio-surveillance and expedited decision-making for casualty management activities, (ii) provide for the upgrade of the EMS Repository to a SaaS; (ii) increase the total not-to-exceed Contract Sum under the Agreement by $6,037,507 to $24,804,395, which includes $787,501 in Pool Dollars for Additional Work, and (iii) provide for other changes set forth herein; and

WHEREAS, Paragraph 6 (Change Notices and Amendments) of the Agreement provides that such changes may be made in the form of an Amendment, which is formally approved and executed by the parties; and

WHEREAS, the Contractor warrants that it continues to possess the competence, expertise and personnel necessary to provide services consistent with the requirements of this Agreement and consistent with the professional standard of care for these services.

NOW, THEREFORE, THE PARTIES HERETO AGREE AS FOLLOWS:

1. This Amendment shall be effective upon execution by all parties.

2. Subparagraph 1.3 (Definitions) of the body of the Agreement is modified to add 1.3.64 amended to read as follows:

   "1.3.64 Additional Work:

   As used herein, the term "Additional Work" shall mean any and all work required by the County and approved pursuant to an Amendment, which includes upgrading the EMS Repository to a SaaS and which shall be provided by Contractor in accordance with Exhibit A.2 (SOW)."

3. Subparagraph 1.3 (Definitions) of the body of the Agreement is modified to add 1.3.65 amended to read as follows:

   "1.3.65 Pool Dollars:

   As used herein, the term "Pool Dollars" shall mean the maximum amount allocated under this Agreement for acquiring Additional Work provided by the Contractor, and approved by the County in accordance with the terms of this Agreement and as set forth in Exhibit B (Schedule of Payments)."

4. Subparagraph 3.5 (Contractor's Staff Identification) of the body of the Agreement is deleted in its entirety and replaced with revised Subparagraph 3.5 (Contractor's Staff Identification) amended to read as follows:

"3.5 CONTRACTOR'S STAFF IDENTIFICATION:

3.5.1 All Contractor staff performing work primarily for the County under this Agreement shall undergo and pass, to the satisfaction of the County, a background investigation as a condition of beginning and continuing to work under this Agreement. The County shall use its discretion in determining the method of background clearance to be used, which may include but is not limited to fingerprinting. The County shall perform the background check.

3.5.2 The County may request that the Contractor's staff members be immediately removed from working on the County Agreement at any time during the term of this Agreement, if such staff member does not pass a background investigation to the satisfaction of the County whose background or conduct is incompatible with the County's facility access. The County will not provide to the Contractor nor to the Contractor's staff any information obtained through the County conducted background clearance unless required by applicable law.

3.5.3 The County may also immediately, at the sole discretion of the County, deny or terminate facility access to the Contractor's staff that do not pass such investigation(s) to the satisfaction of the County whose background or conduct is incompatible with County facility access.

3.5.4 Disqualification, if any, of the Contractor's staff, pursuant to this Subparagraph 3.5, shall not relieve the Contractor of its obligation to complete all work in accordance with the terms and conditions of this Agreement."

5. Paragraph 5 (Term) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 5 (Term) amended to read as follows:

"5. TERM:

5.1 The term of this Agreement shall commence on the Effective Date and shall continue in full force until and through September 30, 2026, unless sooner terminated, in whole or in part, as provided in the Agreement (hereinafter "Initial Term").

5.2 As used throughout this Agreement, the word "term" when referring to the term of the Agreement shall include the Initial Term and Optional Term, to the extent County exercises its term extension options pursuant to this Paragraph 5.

5.3 The County maintains databases that track/monitor Contractor performance history. Information entered into such databases may be used for a variety of purposes, including determining whether County will exercise a term extension option.

5.4 Contractor shall notify County when this Agreement is within six (6) months from the expiration of the term as provided for hereinabove. Upon occurrence of this event, Contractor shall send written notification to County at the address herein

provided in Paragraph 69 (Notices). Notwithstanding the foregoing, Contractor's failure to provide such notification shall not constitute a material breach of this Agreement."

6. Subparagraph 7.1 (General) of the body of the Agreement is deleted in its entirety and replaced with revised Subparagraph 7.1 (General) amended to read as follows:

"7.1 GENERAL:

The Contract Sum under this Agreement shall be the total monetary amount payable by County to Contractor for supplying all the tasks, deliverables, goods, services, and other work requested and specified under this Agreement. All work completed by Contractor must be approved in writing by County. If County does not approve work in writing, no payment shall be due to Contractor for that work. The Contract Sum, including all applicable taxes, authorized by County hereunder for the maximum term of the Agreement shall not exceed Twenty-Four Million, Eight Hundred Four Thousand, Three Hundred Ninety-Five Dollars ($24,804,395). Notwithstanding any provision of this Subparagraph 7.1, Contractor shall fully perform and complete all work required of Contractor by this Agreement in exchange for the amounts to be paid to Contractor as set forth in this Agreement.

The Contract Sum shall not be adjusted for any costs or expenses whatsoever of Contractor."

7. Paragraph 13 (Independent Contractor Status) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 13 (Independent Contractor Status) amended to read as follows:

"13. INDEPENDENT CONTRACTOR STATUS:

13.1 This Agreement is by and between the County and the Contractor and is not intended, and shall not be construed, to create the relationship of agent, servant, employee, partnership, joint venture, or association, as between the County and the Contractor. The employees and agents of one party shall not be, or be construed to be, the employees or agents of the other party for any purpose whatsoever.

13.2 The Contractor shall be solely liable and responsible for providing to, or on behalf of, all persons performing work pursuant to this Agreement all compensation and benefits. The County shall have no liability or responsibility for the payment of any salaries, wages, unemployment benefits, disability benefits, Federal, State, or local taxes, or other compensation, benefits, or taxes for any personnel provided by or on behalf of the Contractor. Consistent with the foregoing, the County shall have no liability, and the Contractor shall be solely and fully liable and responsible, to any of the Contractor's employees, subcontractors or other persons providing work under the Agreement on behalf

of the Contractor, if any such person is unable to work or is required to stop working (permanently or temporarily) as a result of the person's exposure to an infectious disease or other hazard while performing work pursuant to the Agreement, even if such person complied with all applicable Federal, State and local laws, rules, regulations, ordinances, directives, guidelines, policies and procedures, including those relating to the work site. Nothing in this Subparagraph is intended in any way to alter or release Contractor from obligation to obtain and maintain the requisite workers' compensation coverage pursuant to Subparagraph 14.3, C. Workers' Compensation and Employers' Liability.

13.3 The Contractor understands and agrees that all persons performing work pursuant to this Agreement are, for purposes of Workers' Compensation liability, solely employees of the Contractor and not employees of the County. The Contractor shall be solely liable and responsible for furnishing any and all Workers' Compensation benefits to any person as a result of any injuries arising from or connected with any work performed by or on behalf of the Contractor pursuant to this Agreement.

13.4 The Contractor shall adhere to the provisions stated in Paragraph 41. Confidentiality."

8. Subparagraph 14.3 (Insurance Coverage Requirements) of the body of the Agreement is modified by adding Section G to read as follows:

"G. Cyber Liability Insurance:

The Contractor shall secure and maintain cyber liability insurance coverage with limits of $8,000,000 per occurrence and in the aggregate during the term of the Agreement, including coverage for: network security liability; privacy liability; privacy regulatory proceeding, defense, response, expenses and fines; technology professional liability (errors and omissions); privacy breach expense reimbursement (liability arising from the loss or disclosure of County Information no matter how it occurs); system breach; denial or loss of service; introduction, implantation, or spread of malicious software code; unauthorized access to or use of computer systems; and Data/Information loss and business interruption; any other liability or risk that arises out of the Agreement. The Contractor shall add the County as an additional insured to its cyber liability insurance policy and provide to the County certificates of insurance evidencing the foregoing upon the County's request. The procuring of the insurance described herein, or delivery of the certificates of insurance described herein, shall not be construed as a limitation upon the Contractor's liability or as full performance of its indemnification obligations hereunder. No exclusion/restriction for unencrypted portable devices/media may be on the policy so long as such provisions are commercially available on the market."

9. Paragraph 21 (Compliance with Applicable Laws) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 21 (Compliance with Applicable Laws) amended to read as follows:

"21. COMPLIANCE WITH APPLICABLE LAWS:

21.1 In the performance of this Agreement, the Contractor and the County shall each comply with all current and applicable Federal, State and local laws, rules, regulations, ordinances, directives, guidelines, policies and procedures, including, but not limited to standards of The Joint Commission, its National Patient Safety Goals, California Code of Regulations, Title 22, Division 5 regulations and all other applicable industry best practices standards. All provisions required thereby to be included in this Agreement are incorporated herein by reference.

21.2 The Contractor shall indemnify, defend, and hold harmless the County, its officers, employees, agents and volunteers from and against any and all claims, demands, damages, liabilities, losses, administrative penalties and fines assessed, costs, and expenses, including, without limitation, defense costs and legal, accounting and other expert, consulting or professional fees, arising from, connected with, or related to any failure by the Contractor, its officers, employees, agents, or subcontractors, to comply with any such laws, rules, regulations, ordinances, directives, guidelines, policies, or procedures. Any legal defense pursuant to the Contractor's indemnification obligations under this Paragraph 21 shall be conducted by the Contractor and performed by counsel selected by the Contractor and approved by the County. Notwithstanding the preceding sentence, the County shall have the right to participate in any such defense at its sole cost and expense, except that in the event the Contractor fails to provide the County with a full and adequate defense, the County shall be entitled to retain its own counsel, including, without limitation, County Counsel, and reimbursement from the Contractor for all such costs and expenses incurred by the County in doing so. The Contractor shall not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of the County without the County's prior written approval."

10. Paragraph 23 (Nondiscrimination, Affirmative Action, and Assurance of Compliance with Civil Rights Laws) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 23 (Nondiscrimination, Affirmative Action, and Assurance of Compliance with Civil Rights Laws) amended to read as follows:

"23. NONDISCRIMINATION, AFFIRMATIVE ACTION AND ASSURANCE OF COMPLIANCE WITH CIVIL RIGHTS LAWS:

23.1 The Contractor hereby assures that it will comply with Subchapter VI of the Civil Rights Act of 1964, 42 USC Sections 2000 (e) (1) through 2000 (e) (17); the Fair Employment & Housing Act, Government Code Section 12920-12922; and Affirmative Action in County Agreements, Chapter 4.32 of the Los Angeles County Code to the end that no person shall, on the grounds of race, color, religious creed,

ancestry, national origin, sex, sexual orientation, age, physical or mental disability, medical condition, marital status, or political affiliation, be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under this Agreement or under any project, program, or activity supported by this Agreement.

23.2 The Contractor certifies and agrees that all persons employed by it, its affiliates, subsidiaries, or holding companies are and shall be treated equally without regard to or because of race, color, religious creed, ancestry, national origin, sex, sexual orientation, age, physical or mental disability, medical condition, marital status, or political affiliation, in compliance with all applicable Federal and State anti-discrimination laws and regulations.

23.3 The Contractor shall take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to race, color, religious creed, ancestry, national origin, sex, sexual orientation, age, physical or mental disability, medical condition, marital status, or political affiliation, in compliance with all applicable Federal and State anti-discrimination laws and regulations. Such action shall include, but is not limited to: employment, upgrading, demotion, transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.

23.4 The Contractor certifies and agrees that it will deal with its subcontractors, bidders, or vendors without regard to or because of race, color, religious creed, ancestry, national origin, sex, sexual orientation, age, physical or mental disability, medical condition, marital status, or political affiliation.

23.5 The Contractor certifies and agrees that it, its affiliates, subsidiaries, or holding companies shall comply with all applicable Federal and State laws and regulations to the end that no person shall, on the grounds of race, color, religious creed, ancestry, national origin, sex, sexual orientation, age, physical or mental disability, medical condition, marital status, or political affiliation, be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under this Agreement or under any project, program, or activity supported by this Agreement.

23.6 The Contractor shall allow County representatives access to the Contractor's employment records during regular business hours to verify compliance with the provisions of this Paragraph 23 when so requested by the County.

23.7 If the County finds that any provisions of this Paragraph 23 have been violated, such violation shall constitute a material breach of this Agreement upon which the County may terminate or suspend this Agreement. While the County reserves the right to determine independently that the anti-discrimination provisions of this Agreement have been violated, in addition, a determination by the California Fair Employment Practices Commission or the Federal Equal Employment Opportunity Commission that the Contractor has violated Federal or State anti-discrimination laws or regulations shall constitute a finding by the County that the Contractor has violated the anti-discrimination provisions of this Agreement.

23.8 The parties agree that in the event the Contractor violates any of the anti-discrimination provisions of this Agreement, the County shall, at its sole option, be entitled to the sum of Five Hundred Dollars ($500) for each such violation pursuant to California Civil Code Section 1671 as liquidated damages in lieu of terminating or suspending this Agreement.

23.9 The Contractor shall certify to, and comply with, the provisions of Exhibit D (Contractor's EEO Certification)."

11. Paragraph 24 (Employment Eligibility Verification) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 24 (Employment Eligibility Verification) amended to read as follows:

"24 EMPLOYMENT ELIGIBILITY VERIFICATION:

24.1 The Contractor warrants that it fully complies with all Federal and State statutes and regulations regarding the employment of aliens and others and that all its employees performing work under this Agreement meet the citizenship or alien status requirements set forth in Federal and State statutes and regulations. The Contractor shall obtain, from all employees performing work hereunder, all verification and other documentation of employment eligibility status required by Federal and State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, (P.L. 99-603), or as they currently exist and as they may be hereafter amended. The Contractor shall retain all such documentation for all covered employees for the period prescribed by law.

24.2 The Contractor shall indemnify, defend, and hold harmless, the County, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against the Contractor or the County or both in connection with any alleged violation of any Federal or State statutes or regulations pertaining to the eligibility for employment of any persons performing work under this Agreement."

12. Paragraph 29 (Termination for Insolvency) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 29 (Termination for Insolvency) amended to read as follows:

"29. TERMINATION FOR INSOLVENCY:

29.1 The County may terminate this Agreement forthwith in the event of the occurrence of any of the following:

- Insolvency of the Contractor. The Contractor shall be deemed to be insolvent if it has ceased to pay its debts for at least sixty (60) days in the ordinary course of business or cannot pay its debts as they become due, whether or not a petition has been filed under the Federal Bankruptcy Code and whether or not the Contractor is insolvent within the meaning of the Federal Bankruptcy Code;

- The filing of a voluntary or involuntary petition regarding the Contractor under the Federal Bankruptcy Code;
- The appointment of a Receiver or Trustee for the Contractor; or
- The execution by the Contractor of a general assignment for the benefit of creditors.

29.2 The rights and remedies of the County provided in this Paragraph 29 shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Agreement."

13. Paragraph 33 (Prohibition Against Subcontracting) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 33 (Subcontracting) amended to read as follows:

"33. SUBCONTRACTING:

33.1 The requirements of this Agreement may not be subcontracted by the Contractor **without the advance written approval of the County**. Any attempt by the Contractor to subcontract without the prior consent of the County may be deemed a material breach of this Agreement.

33.2 If the Contractor desires to subcontract, the Contractor shall provide the following information promptly at the County's request:

- A description of the work to be performed by the subcontractor;
- A draft copy of the proposed subcontract; and
- Other pertinent information and/or certifications requested by the County.

33.3 The Contractor shall indemnify and hold the County harmless with respect to the activities of each and every subcontractor in the same manner and to the same degree as if such subcontractor(s) were the Contractor employees.

33.4 The Contractor shall remain fully responsible for all performances required of it under this Agreement, including those that the Contractor has determined to subcontract, notwithstanding the County's approval of the Contractor's proposed subcontract.

33.5 The County's consent to subcontract shall not waive the County's right to prior and continuing approval of any and all personnel, including subcontractor employees, providing services under this Agreement. The Contractor is responsible to notify its subcontractors of this County right.

33.6 The Director or designee is authorized to act for and on behalf of the County with respect to approval of any subcontract and subcontractor employees. After approval

of the subcontract by the County, the Contractor shall forward a fully executed subcontract to the County for its files.

33.7 The Contractor shall be solely liable and responsible for all payments or other compensation to all subcontractors and their officers, employees, agents, and successors in interest arising through services performed hereunder, notwithstanding the County's consent to subcontract.

33.8 The Contractor shall obtain certificates of insurance, which establish that the subcontractor maintains all the programs of insurance required by the County from each approved subcontractor. The Contractor shall ensure delivery of all such documents to the Certificate Holder, at:

cgcontractorinsurance@dhs.lacounty.gov

before any subcontractor employee may perform any work hereunder."

14. Paragraph 35 (Notice of Delays) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 35 (Notice of Delays) amended to read as follows:

"35. NOTICE OF DELAYS:

Except as otherwise provided under this Agreement, when either party has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this Agreement, that party shall, within one (1) business day, give notice thereof, including all relevant information with respect thereto, to the other party."

15. Paragraph 39 (Unlawful Solicitation) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 39 (Unlawful Solicitation) amended to read as follows:

"39. UNLAWFUL SOLICITATION:

The Contractor shall inform all of its officers and employees performing services hereunder of the provisions of Article 9 of Chapter 4 of Division 3 (commencing with section 6150) of Business and Professions Code of the State of California (i.e. State Bar Act provisions regarding unlawful solicitation as a runner or capper for attorneys) and shall take positive and affirmative steps in its performance hereunder to ensure that there is no violation of said provisions by its officers and employees. The Contractor agrees that if a patient requests assistance in obtaining the services of any attorney, it will refer the patient to the attorney referral service of all those bar associations within Los Angeles County that have such a service."

16. Subparagraph 41.1 (Confidentiality) of the body of the Agreement is deleted in its entirety and replaced with revised Subparagraph 41.1 amended to read as follows:

"41.1 Confidentiality:

41.1.1 The Contractor shall maintain the confidentiality of all records, data, and information, including, but not limited to, billings, the County records, TEMIS Data, and patient records ("County Confidential Information"), in accordance with all applicable Federal, State and local laws, rules, regulations, ordinances, directives, guidelines, policies and procedures relating to confidentiality, including, without limitation, the County policies concerning information technology security and the protection of confidential records and information.

41.1.2 Furthermore, the Contractor shall: (i) not use any such records or information for any purpose whatsoever other than carrying out the express terms of this Agreement; (ii) promptly transmit to the County all requests for disclosure of any such records or information; (iii) not disclose, except as otherwise specifically permitted by this Agreement, any such records or information to any person or organization other than the County without the County's prior written authorization that the information is releasable; and (iv) at the expiration or termination of this Agreement, return all such records and information to the County or maintain such records and information in accordance with the written procedures that may be provided or made available to the Contractor by the County for this purpose.

41.1.3 All County Confidential Information is deemed property of the County, and the County shall retain exclusive rights and ownership thereto. County Confidential Information shall not be used by the Contractor for any purpose other than as required under this Agreement, nor shall such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by the Contractor, or commercially exploited or otherwise used by, or on behalf of, the Contractor, its officers, directors, employees, or agents. The Contractor may assert no lien on or right to withhold from the County, any County Confidential Information it receives from, receives addressed to, or stores on behalf of, the County.

41.1.4 The Contractor acknowledges and agrees that due to the unique nature of County Confidential Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach may result in irreparable harm to the County, and therefore, that upon any such breach, the County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies are available within law or equity. Any breach of Subparagraph 41.1 (Confidentiality) shall constitute a material breach of this Agreement and be grounds for immediate termination of this Agreement in the exclusive discretion of the County.

41.1.5 The Contractor shall indemnify, defend, and hold harmless the County, its Special Districts, elected and appointed officers, employees, and agents, from and against any and all claims, demands, damages, liabilities, losses, costs and expenses,

administrative penalties and fines assessed including, without limitation, defense costs and legal, accounting and other expert, consulting, or professional fees, arising from, connected with, or related to any failure by the Contractor, its officers, employees, agents, or subcontractors, to comply with this Paragraph 41. Any legal defense pursuant to the Contractor's indemnification obligations under this Paragraph 41 shall be conducted by the Contractor and performed by counsel selected by the Contractor and approved by the County. Notwithstanding the preceding sentence, the County shall have the right to participate in any such defense at its sole cost and expense, except that in the event the Contractor fails to provide the County with a full and adequate defense, the County shall be entitled to retain its own counsel, including, without limitation, County Counsel, and reimbursement from the Contractor for all such costs and expenses incurred by the County in doing so. The Contractor shall not have the right to enter into any settlement, agree to any injunction, or make any admission, in each case, on behalf of the County without the County's prior written approval.

41.1.4 The Contractor shall inform all of its officers, employees, agents and subcontractors whose roles are primarily dedicated to providing the County services hereunder of the confidentiality and indemnification provisions of this Agreement.

41.1.5 The Contractor shall cause each employee whose role is primarily dedicated to performing services covered by this Agreement to the County to sign and adhere to the provisions of the Exhibit C - Contractor Employee Acknowledgment, and Confidentiality Agreement.

41.1.6 The Contractor shall cause each non-employee whose role is primarily dedicated to performing services covered by this Agreement to the County to sign and adhere to the provisions of the Exhibit C.1 - Contractor Non-Employee Acknowledgment, and Confidentiality Agreement."

17. Paragraph 52 (Contractor Performance During Civil Unrest and Disaster) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 52 (Contractor Performance During Civil Unrest and Disaster) amended to read as follows:

"52. <u>CONTRACTOR PERFORMANCE DURING CIVIL UNREST AND DISASTER:</u>

The Contractor recognizes that health care Facilities maintained by the County provide care essential to the residents of the communities they serve, and that these services are of particular importance at the time of a riot, insurrection, civil unrest, natural disaster, or similar event. Notwithstanding any other provision of this Agreement, full performance by the Contractor during any riot, insurrection, civil unrest, natural disaster or similar event is not excused if such performance remains physically possible. Failure to comply with this requirement shall be considered a material breach by the Contractor for which the County may immediately terminate this Agreement."

18. Paragraph 53 (Contractor's Warranty of Adherence to County's Child Support Compliance Program) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 53 (Contractor's Warranty of Adherence to County's Child Support Compliance Program) amended to read as follows:

"53. CONTRACTOR'S WARRANTY OF ADHERENCE TO COUNTY'S CHILD SUPPORT COMPLIANCE PROGRAM:

53.1 The Contractor acknowledges that the County has established a goal of ensuring that all individuals who benefit financially from the County through contract are in compliance with their court-ordered child, family and spousal support obligations in order to mitigate the economic burden otherwise imposed upon the County and its taxpayers.

53.2 As required by the County's Child Support Compliance Program (County Code Chapter 2.200) and without limiting the Contractor's duty under this Agreement to comply with all applicable provisions of law, the Contractor warrants that it is now in compliance and shall during the term of this Agreement maintain in compliance with employment and wage reporting requirements as required by the Federal Social Security Act (42 USC Section 653a) and California Unemployment Insurance Code Section 1088.5, and shall implement all lawfully served Wage and Earnings Withholding Orders or Child Support Services Department Notices of Wage and Earnings Assignment for Child, Family or Spousal Support, pursuant to Code of Civil Procedure Section 706.031 and Family Code Section 5246(b)."

19. Paragraph 54 (Termination for Breach of Warranty to Maintain Compliance with County's Child Support Compliance Program) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 54 (Contractor's Warranty of Adherence to County's Child Support Compliance Program) amended to read as follows:

"54. TERMINATION FOR BREACH OF WARRANTY TO MAINTAIN COMPLIANCE WITH COUNTY'S CHILD SUPPORT COMPLIANCE PROGRAM:

Failure of the Contractor to maintain compliance with the requirements set forth in Paragraph 53 - Contractor's Warranty of Adherence to County's Child Support Compliance Program, shall constitute default under this Agreement. Without limiting the rights and remedies available to the County under any other provision of this Agreement, failure of the Contractor to cure such default within ninety (90) calendar days of written notice shall be grounds upon which the County may terminate this Agreement pursuant to Paragraph 30 - Termination for Default and pursue debarment of the Contractor, pursuant to County Code Chapter 2.202."

20. Paragraph 61 (Licenses, Permits. Registrations, Accreditations and Certificates) of the body of the Agreement is deleted in its entirety and replaced with revised Paragraph 61 (Licenses, Permits. Registrations, Accreditations and Certificates) amended to read as follows:

"61. LICENSES, PERMITS. REGISTRATIONS, ACCREDITATIONS AND CERTIFICATES:

The Contractor shall obtain and maintain in effect during the term of this Agreement, all valid licenses, permits, registrations, accreditations, and certificates required by law which are applicable to its performance of this Agreement, and shall ensure that all of its officers, employees, and agents who perform services hereunder obtain and maintain in effect during the term of this Agreement, all licenses, permits, registrations, accreditations, and certificates required by law which are applicable to their performance of services hereunder. All such licenses, permits, registrations, accreditations, and certifications relating to services hereunder shall be made available to the County upon request."

21. Paragraph 91 (Complaints) is added to the body of the Agreement to read as follows:

"91. COMPLAINTS:

The Contractor shall develop, maintain and operate procedures for receiving, investigating and responding to complaints.

91.1 Within (twenty) (20) business days after Agreement effective date, the Contractor shall provide the County with the Contractor's policy for receiving, investigating and responding to user complaints.

91.2 The County will review the Contractor's policy and provide the Contractor with approval of said plan or with requested changes.

91.3 If the County requests changes in the Contractor's policy, the Contractor shall make such changes and resubmit the plan within (five) (5) business days for the County approval.

91.4 If, at any time, the Contractor wishes to change the Contractor's policy, the Contractor shall submit proposed changes to the County for approval before implementation.

91.5 The Contractor shall preliminarily investigate all complaints and notify the Facility's Project Manager of the status of the investigation within (ten) (10) business days of receiving the complaint.

91.6 When complaints cannot be resolved informally, a system of follow-through shall be instituted which adheres to formal plans for specific actions and strict time deadlines.

91.7 Copies of all written responses shall be sent to the Facility's Project Manager within (ten) (10) business days of mailing to the complainant."

22. Paragraph 92 (Consideration of Hiring County Employees Targeted for Layoff or are on a County Re-Employment List) is added to the body of the Agreement to read as follows:

"92. CONSIDERATION OF HIRING COUNTY EMPLOYEES TARGETED FOR LAYOFF OR ARE ON A COUNTY RE-EMPLOYMENT LIST:

Should the Contractor require additional or replacement personnel after the effective date of this Agreement to perform the services set forth herein, the Contractor shall give first consideration for such employment openings to qualified, permanent County employees who are targeted for layoff or qualified, former County employees who are on a re-employment list during the life of this Agreement."

23. Paragraph 93 (Health Insurance Portability and Accountability Act of 1996 (HIPAA)) is added to the body of the Agreement to read as follows:

"93. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA):

The County is subject to the Administrative Simplification requirements and prohibitions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), and regulations promulgated thereunder, including the Privacy, Security, Breach Notification, and Enforcement Rules at 45 Code of Federal Regulations (C.F.R.) Parts 160 and 164 (collectively, the "HIPAA Rules"). Under this Agreement, the Contractor provides services to the County and the Contractor creates, has access to, receives, maintains, or transmits Protected Health Information as defined in Exhibit L in order to provide those services. The County and the Contractor therefore agree to the terms of Exhibit L - Business Associate Under Health Insurance Portability and Accountability Act of 1996 (HIPAA)."

24. Paragraph 94 (Non Exclusivity) is added to the body of the Agreement to read as follows:

"94. NON EXCLUSIVITY:

Nothing herein is intended nor shall be construed as creating any exclusive arrangement with the Contractor. This Agreement shall not restrict the Department of Health Services from acquiring similar, equal or like goods and/or services from other entities or sources."

25. Paragraph 95 (Notice of Disputes) is added to the body of the Agreement to read as follows:

"95. NOTICE OF DISPUTES:

The Contractor shall bring to the attention of the Facility's Project Manager and/or Facility's Project Director any dispute between the County and the Contractor regarding the performance of services as stated in this Agreement. If the Facility's Project Manager or Facility's Project Director is not able to resolve the dispute, the Director or designee shall resolve it."

26. Paragraph 96 (Prohibition Against Inducement or Persuasion) is added to the body of the Agreement to read as follows:

"96. PROHIBITION AGAINST INDUCEMENT OR PERSUASION:

Notwithstanding the above, the Contractor and the County agree that, during the term of this Agreement and for a period of one year thereafter, neither party shall in any way intentionally induce or persuade any employee of one party to become an employee or agent of the other party. No bar exists against any hiring action initiated through a public announcement."

27. Paragraph 97 (Public Records Act) is added to the body of the Agreement to read as follows:

"97. PUBLIC RECORDS ACT:

97.1 Any documents submitted by the Contractor; all information obtained in connection with the County's right to audit and inspect the Contractor's documents, books, and accounting records pursuant to Paragraph 99 - Record Retention and Inspection/Audit Settlement of this Agreement; as well as any documents that may have been submitted in response to a solicitation process for this Agreement, become the exclusive property of the County. All such documents become a matter of public record and shall be regarded as public records. Exceptions will be those elements in the California Government Code Section 6250 et seq. (Public Records Act) and which are marked "trade secret", "confidential", or "proprietary". The County shall not in any way be liable or responsible for the disclosure of any such records including, without limitation, those so marked, if disclosure is required by law, or by an order issued by a court of competent jurisdiction.

97.2 In the event the County is required to defend an action on a Public Records Act request for any of the aforementioned documents, information, books, records, and/or contents of a proposal marked "trade secret", "confidential", or "proprietary", the Contractor agrees to defend and indemnify the County from all costs and expenses, including reasonable attorney's fees, in an action or liability arising under the Public Records Act."

28. Paragraph 98 (Publicity) is added to the body of the Agreement to read as follows:

"98. PUBLICITY:

98.1 The Contractor shall not disclose any details in connection with this Agreement to any person or entity except as may be otherwise provided hereunder or required by law. However, in recognizing the Contractor's need to identify its services and related clients to sustain itself, the County shall not inhibit the Contractor from publishing its role under this Agreement within the following conditions:

- The Contractor shall develop all publicity material in a professional manner; and

- During the term of this Agreement, the Contractor shall not, and shall not authorize another to, publish or disseminate any commercial advertisements, press releases, feature articles, or other materials using the name of the County without the prior written consent of the Director or designee. The County shall not unreasonably withhold written consent.

98.2 The Contractor may, without the prior written consent of the County, indicate in its proposals and sales materials that it has been awarded this Agreement with the County of Los Angeles, provided that the requirements of this Paragraph 98 shall apply."

29. Paragraph 99 (Record Retention and Inspection/Audit Settlement) is added to the body of the Agreement to read as follows:

"99. RECORD RETENTION AND INSPECTION/AUDIT SETTLEMENT:

99.1 The Contractor shall maintain, and provide upon request by the County, accurate and complete financial records of its activities and operations relating to this Agreement in accordance with generally accepted accounting principles. The Contractor shall also maintain accurate and complete employment and other records relating to its performance of this Agreement.

99.2 The Contractor agrees that the County, or its authorized representatives, shall have access to and the right to examine, audit, excerpt, copy, or transcribe any pertinent transaction, activity, or record relating to this Agreement. All such material, including, but not limited to, all financial records, bank statements, cancelled checks or other proof of payment, timecards, sign-in/sign-out sheets and other time and employment records, and proprietary data and information, shall be kept and maintained by the Contractor and shall be made available to the County during the term of this Agreement and for a period of five (5) years thereafter unless the County's written permission is given to dispose of any such material prior to such time.

99.3 In the event that an audit of the Contractor is conducted specifically regarding this Agreement by any Federal or State auditor, or by any auditor or accountant

employed by the Contractor or otherwise, including audits conducted by the Medicare and Medi-Cal programs, or both, then the Contractor shall file a copy of each such audit report, including Service Organization Controls (SOC1) Reports, with the County's Auditor-Controller within thirty (30) days of the Contractor's receipt thereof, unless otherwise provided by applicable Federal or State law or under this Agreement. Subject to applicable law, the County shall make a reasonable effort to maintain the confidentiality of such audit report(s).

99.4 Failure on the part of the Contractor to comply with any of the provisions of this Paragraph 99 shall constitute a material breach of this Agreement upon which the County may terminate or suspend this Agreement.

99.5 If, at any time during the term of this Agreement or within five (5) years after the expiration or termination of this Agreement, representatives of the County conduct an audit of the Contractor regarding the work performed under this Agreement, and if such audit finds that the County's dollar liability for any such work is less than payments made by the County to the Contractor, then the difference shall be either: a) repaid by the Contractor to the County by cash payment upon demand or b) at the sole option of the County's Auditor-Controller, deducted from any amounts due to the Contractor from the County, whether under this Agreement or otherwise. If such audit finds that the County's dollar liability for such work is more than the payments made by the County to the Contractor, then the difference shall be paid to the Contractor by the County by cash payment, provided that in no event shall the County's maximum obligation for this Agreement exceed the funds appropriated by the County for the purpose of this Agreement."

30. Paragraph 100 (Recycled Bond Paper) is added to the body of the Agreement to read as follows:

"100. RECYCLED BOND PAPER:

Consistent with the Board of Supervisors' policy to reduce the amount of solid waste deposited at the County landfills, the Contractor agrees to use recycled-content paper to the maximum extent possible on this Agreement."

31. Paragraph 101 (Termination for Non-Appropriation of Funds) is added to the body of the Agreement to read as follows:

"101. TERMINATION FOR NON-APPROPRIATION OF FUNDS:

Notwithstanding any other provision of this Agreement, the County shall not be obligated for the Contractor's performance hereunder or by any provision of this Agreement during any of the County's future fiscal years unless and until the County's Board of Supervisors appropriates funds for this Agreement in the County's Budget for each such future fiscal year. In the event that funds are not appropriated for this Agreement, then this Agreement shall terminate as of September 30 of the last fiscal year for which funds were appropriated. The

County shall notify the Contractor in writing of any such non-allocation of funds at the earliest possible date."

32. Paragraph 102 (SaaS Limitation of Liability) is added to the body of the Agreement to read as follows:

"102. SAAS LIMITATIONS OF LIABILITY:

Notwithstanding any other provision of this Agreement, with respect to the services delivered pursuant to Exhibit A.2 (Statement of Work – EMS Repository):

102.1 NEITHER CONTRACTOR NOR COUNTY SHALL BE LIABLE TO THE OTHER FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, PUNITIVE OR INCIDENTAL DAMAGES, INCLUDING CLAIMS FOR DAMAGES FOR LOST PROFITS, GOODWILL, USE OF MONEY, INTERRUPTED OR IMPAIRED USE OF THE SOFTWARE, AVAILABILITY OF DATA, STOPPAGE OF WORK OR IMPAIRMENT OF OTHER ASSETS RELATING TO THIS AGREEMENT.

102.2 EXCEPT TO THE EXTENT ARISING FROM CONTRACTOR OR COUNTY'S WILLFUL MISCONDUCT OR CRIMINAL CONDUCT, EACH OF CONTRACTOR'S AND COUNTY'S MAXIMUM AGGREGATE LIABILITY FOR ALL CLAIMS OF LIABILITY ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT SHALL NOT EXCEED $9,000,000."

33. Exhibit A.2 (Statement of Work – EMS Repository) is added to the Agreement, which is attached hereto as Attachment 1 and incorporated herein by reference. References to Exhibit A in the Agreement shall include Exhibit A.2 (Statement of Work – EMS Repository) and references to attachments, tasks, and deliverables, and paragraphs of Exhibit A (Statement of Work) in the Agreement shall mean, where applicable, references to the equivalent item in Exhibit A.2 (Statement of Work – EMS Repository). The pages of Exhibit A.2 (Statement of Work – EMS Repository) are each designated at the bottom as "Added Under Amendment Number Twelve."

34. Exhibit B (Schedule of Payments) is deleted in its entirety and replaced with revised Exhibit B (Schedule of Payments), which is attached hereto as Attachment 2 and incorporated herein by reference. The pages of revised Exhibit B (Schedule of Payments) are each designated at the bottom as "Revised Under Amendment Number Twelve."

35. Exhibit C (Contractor Employee Acknowledgment, Confidentiality, and Copyright Assignment Agreement) is deleted in its entirety and replaced with revised Exhibit C (Contractor Employee Acknowledgment and Confidentiality Agreement), Exhibit C.1 (Contractor Non-Employee Acknowledgement and Confidentiality Agreement), which are attached hereto as Attachment 3 and incorporated herein by reference. The pages of revised Exhibit C (Contractor Employee Acknowledgment and Confidentiality Agreement), Exhibit C.1 (Contractor Non-Employee Acknowledgement and

Confidentiality Agreement) are each designated at the bottom as "Revised Under Amendment Number Twelve."

36. Exhibit L (Business Associate Agreement under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)), is deleted in its entirety and replaced with revised Exhibit L (Business Associate Agreement under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)), which is attached hereto as Attachment 4 and incorporated herein by reference. The pages of revised Exhibit L (Business Associate Agreement under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)) are each designated at the bottom as "Revised Under Amendment Number Twelve."

37. Exhibit M (Information Security Requirements) is added to the Agreement, which is attached hereto as Attachment 5 and incorporated herein by reference.

38. Except for the changes set forth hereinabove, the Agreement shall not be changed in any respect by this Amendment.

/
/
/

IN WITNESS WHEREOF, the Board of Supervisors of the County of Los Angeles has caused this Amendment to be executed by the County's Director of Health Services, or authorized designee, and Contractor has caused this Amendment to be executed on its behalf by its duly authorized officer(s), on the day, month, and year first above written.

COUNTY OF LOS ANGELES

By:_____for
Christina R. Ghaly, M.D.
Director of Health Services

CONTRACTOR

ESO SOLUTIONS, INC.

By:_____
Signature

_____
Printed Name

_____
Title

APPROVED AS TO FORM:
DAWYN HARRISON
County Counsel

By:_____
Truc Moore
Principal Deputy County Counsel

EXHIBIT A.2

STATEMENT OF WORK
EMS REPOSITORY

(ADDED UNDER AMENDMENT TWELVE)

SEPTEMBER 2023

TABLE OF CONTENTS

1. GENERAL

1.1 INTRODUCTION

CONTRACTOR is currently providing the COUNTY with an integrated Trauma and Emergency Medicine Information System (TEMIS). The TEMIS consists of four data registries, the EMS Repository, LA Fire Rescue, LA Base, and LA Trauma.

This Statement of Work only covers the upgrade of the EMS Repository to a software platform hosted by the CONTRACTOR in the cloud and accessible over the Internet via a website (commonly referred to as software-as-a-service (SaaS)) to gather real-time EMS incident and patient level data. CONTRACTOR will provide the COUNTY with a cloud-based and fully hosted system for the EMS Repository, to be referred to as "EMS Repository NEMSIS Standard" ("EMS Repository" or "SaaS Platform"). This will upgrade the client-based legacy LA Fire-Rescue data registry. LA Fire-Rescue is one of four data registries of the COUNTY's TEMIS that is utilized to collect patient level information and patient care provided by EMS provider agencies (fire departments and ambulance operators) to patients in the pre-hospital setting.

TEMIS' other three data registries are utilized to collect hospital related data of patients transported via the 9-1-1 system to analyze health information necessary for EMS system management and to meet COUNTY, State and Federal reporting requirements. TEMIS information is also utilized to share significant information between EMS provider agencies, 9-1-1 receiving facilities, and the COUNTY. CONTRACTOR will continue to provide and support the other three data registries (LA Fire Rescue, LA Base, and LA Trauma) as required by the Agreement until full transition to SaaS, with future statements of work covering such upgrade to SaaS to be negotiated by CONTRACTOR and COUNTY. References to EMS Repository herein will be to the SaaS Platform, and the currently existing EMS Repository that is being upgraded to the SaaS Platform by CONTRACTOR will be referred to as "Legacy System." EMS Repository will be compliant and certified with the most current National Emergency Medical Services Information System (NEMSIS) standards and specifications.

1.2 OVERVIEW

This Statement of Work (SOW) consists of instructions, tasks, subtasks, deliverables, goods, services and other work.

CONTRACTOR shall perform all Tasks and Subtasks associated with the services set forth in this SOW and shall provide all associated Deliverables within the timeframes specified in the Project Work Plan and the applicable Implementation Timeline.

The services set forth in this SOW will be successfully completed upon delivery of a sufficiently user tested, fully functional System that meets the requirements and legal mandates of the COUNTY as detailed in the Agreement, while addressing all

functions and requirements described or referenced within this SOW and all applicable Attachments to this SOW.

CONTRACTOR shall perform, complete and deliver all tasks, subtasks, deliverables, goods, services and other work, however denoted, as set forth in this SOW. Also, defined herein are those Tasks and Subtasks that involve participation of both CONTRACTOR and the COUNTY. Unless otherwise specified as an obligation of the COUNTY, CONTRACTOR shall perform all Tasks and Subtasks and provide all Deliverables as defined herein.

1.3 DEFINITIONS

The terms defined below may be used throughout this SOW and the applicable Attachment to this SOW and shall take precedence in interpretation over the terms defined elsewhere in the Agreement.

1.3.1 Acceptance Test shall mean the COUNTY's written approval of any tasks, subtasks, deliverable, goods, services, or other work provided by CONTRACTOR to COUNTY pursuant to this SOW.

1.3.2 Conference(s) shall have the meaning specified in Subtask 1.2 – Prepare Status Reports and Conduct Conferences.

1.3.3 Final Acceptance Test shall have the meaning specified in Task 5 – Conduct Acceptance Test.

1.3.4 Functional Test shall mean the Acceptance Test to verify the System's compliance with the functional requirements, including the applicable Specifications.

1.3.5 Go-Live shall mean receiving and processing data through the EMS Repository and utilization of CONTRACTOR's reporting platform by authorized COUNTY users for live operation of COUNTY authorized users following the CONTRACTOR's completion and COUNTY's approval of implementation services with regards to the EMS Repository and CONTRACTOR's reporting platform.

1.3.6 Implementation Timeline shall mean the timeline for the implementation of the EMS Repository, as provided in Attachment G.2 (EMS Repository Implementation Timeline).

1.3.7 Integrated System Test shall mean the Acceptance Test to verify that the EMS Repository, including all of its software modules and interfaces, operates in an integrated manner and meets the system requirements of the EMS Repository.

1.3.8 NEMSIS Compliance shall mean TEMIS is certified to the current data standards and specifications established by the National Emergency Medical Services Information System to receive, store and transmit EMS data.

1.3.9 Project shall have the same meaning as implementation of EMS Repository.

1.3.10 Project Work Plan shall have the meaning specified in Subtask 1.1 – Develop Project Work Plan.

1.3.11 Schematron shall mean the rule-based validation language used to validate an Extensible Markup Language (XML) document.

1.3.12 Standard Test Plan shall have the meaning specified in Task 3 – Conduct Acceptance Test for EMS Repository.

1.3.13 Status Report(s) shall have the meaning specified in Subtask 1.2 – Prepare Status Reports and Conduct Conferences.

1.3.14 System Performance Test shall mean the Acceptance Test to verify the EMS Repository's compliance with the system performance requirements of the EMS Repository, including the applicable Specifications.

Capitalized terms used in this SOW without definitions shall have the meanings given to such terms in the body of the Agreement or any of the applicable Attachments to this SOW.

2 SCOPE OF WORK

The sequence in which tasks, subtasks and deliverables appear in this Section 2 of the SOW does not dictate the order in which such tasks, subtasks and deliverables may actually be performed. Unless specified otherwise by the COUNTY, while performing all Tasks and Deliverables listed below in this Section 2 of this SOW, CONTRACTOR shall provide documentation and knowledge transfer relating to such Tasks and Deliverables based on the COUNTY's specifications.

TASK 1 – PROJECT ADMINISTRATION

CONTRACTOR shall provide management and administration for the Project.

SUBTASK 1.1 – DEVELOP PROJECT WORK PLAN

CONTRACTOR shall review the Project requirements for the implementation of the EMS Repository, including the functional specifications and system performance requirements, with the COUNTY's Project Director and the COUNTY's Project Manager. Based upon that review, CONTRACTOR shall prepare a work plan for the Project (hereinafter "Project Work Plan") and submit it for written approval to the COUNTY's Project Director. CONTRACTOR shall update the Project Work Plan to include a detailed work plan for the implementation and testing of the EMS Repository, including, without limitation:

1. A list of milestones, major tasks, associated detailed tasks and associated deliverables.

2. Identification of milestones, tasks and associated deliverables requiring Acceptance by the COUNTY's Project Director upon achievement.

3. Identification of any resources to be provided by the COUNTY.

DELIVERABLE 1.1 – PROJECT WORK PLAN

CONTRACTOR shall deliver to the COUNTY a Project Work Plan prepared in accordance with Subtask 1.1 – Develop Project Work Plan. The Project Work Plan shall provide the basis for the EMS Repository services provided by CONTRACTOR under this Agreement, implementation, configuration and testing of SaaS Platform, including data conversion and migration, and any necessary training. Subsequent to the COUNTY's Project Director's approval, the Project Work Plan may be modified only if such modification has been approved in advance in writing by the COUNTY's Project Director or the COUNTY's Project Manager, as applicable.

CONTRACTOR shall, in accordance with the COUNTY's requirements, address the following major Tasks in the Project Work Plan:

Task 1 - Project Administration

Task 2 - Build and Implement the EMS Repository

Task 3 - Conduct Acceptance Tests for EMS Repository

Task 4 - Archive data in legacy data registry LA Fire Rescue

SUBTASK 1.2 – PREPARE STATUS REPORTS AND CONDUCT CONFERENCES

CONTRACTOR's Project Manager shall provide full project management and control of all Project activities during performance of all tasks set forth in this SOW. This task shall include, but not be limited to:

1. Planning and direction;

2. CONTRACTOR's staffing and personnel matters, including management of CONTRACTOR's technical staff;

3. Evaluation of results and status reporting;

4. Incorporation of the COUNTY's business and technical requirements;

5. Incorporation of required software modifications;

6. Management and tracking of all issues related to the Project.

CONTRACTOR's Project Manager and the COUNTY's Project Manager shall provide reports of Project status (hereinafter "Status Report(s)") on a regular basis and shall participate in regular status meetings and/or teleconferences (hereinafter

"Conference(s)"). The Project and reporting procedures shall include, but not be limited to, the following components:

1. Updated Project Work Plan;

2. Status Reports and Conferences.

The Status Reports prepared by CONTRACTOR's Project Manager pursuant to this Subtask 1.2 – Prepare Status Reports and Conduct Conferences shall be used as the mechanism for CONTRACTOR to report any Project risks or problems identified as part of the implementation process.

DELIVERABLE 1.2 – STATUS REPORTS AND CONFERENCES

CONTRACTOR's Project Manager shall prepare and present to the COUNTY's Project Manager mutually acceptable written Status Reports documenting Project progress, plans, conferences and outstanding issues in accordance with Subtask 1.2 – Prepare Status Reports and Conduct Conferences. CONTRACTOR's Project Manager shall meet with or conduct a status update phone/conference call with the COUNTY's Project Manager at least monthly to review these Project Status Reports and any related matters. All variances shall be presented for approval at the status meeting. The first report shall be presented to the COUNTY's Project Manager one (1) calendar month following the full execution of this Amendment, in a format approved by the COUNTY.

TASK 2 – BUILD AND IMPLEMENT THE EMS REPOSITORY (SAAS PLATFORM)

SUBTASK 2.1 – PROVIDE HARDWARE SPECIFICATIONS FOR ACCESSING EMS REPOSITORY

CONTRACTOR shall provide hardware specifications to access EMS Repository.

DELIVERABLE 2.1 – HARDWARE SPECIFICATIONS

CONTRACTOR shall provide in writing the hardware specifications to access EMS Repository in Subtask 2.1 and certify in writing that the COUNTY provided hardware comply with such specifications.

SUBTASK 2.2 – DEVELOP A SCHEMATRON FOR THE EMS REPOSITORY

CONTRACTOR shall develop a Schematron for the EMS Repository. CONTRACTOR shall assist COUNTY in developing a specific data dictionary defining each specific data variables and calculated fields contained in the EMS Repository.

DELIVERABLE 2.2 – SCHEMATRON FOR THE EMS REPOSITORY

CONTRACTOR shall submit in writing a listing of all data variables in the EMS Repository to the COUNTY and certify in writing that the EMS Repository Schematron is built and ready for publication.

SUBTASK 2.3 – PROVIDE SCHEMATRON FOR PUBLICATION

CONTRACTOR shall provide the COUNTY the Schematron for the EMS Repository in order for COUNTY to publish the Schematron to Los Angeles County EMS provider agencies.

DELIVERABLE 2.3 – SCHEMATRON FOR PUBLICATION

CONTRACTOR shall provide COUNTY with the Schematron for the EMS Repository for publication.

SUBTASK 2.4 – DEVELOP EMS REPOSITORY COMPLIANT WITH NEMSIS STANDARDS

CONTRACTOR shall develop an EMS Repository that is compliant with the latest NEMSIS Standards that is capable of successfully receiving data from EMS provider agencies and exporting NEMSIS compliant data to the California Emergency Medical Services Information System (CEMSIS) in the version requested by CEMSIS.

DELIVERABLE 2.4 – EMS REPOSITORY COMPLIANT WITH NEMSIS STANDARDS

CONTRACTOR shall provide COUNTY written documentation verifying that the EMS Repository is certified to Receive and Process at the latest NEMSIS Standards.

SUBTASK 2.5 – RECEIVE AND PROCESS NEMSIS-COMPLIANT DATA FROM EMS PROVIDER AGENCIES

The EMS Repository shall receive and import NEMSIS- compliant data from EMS provider agencies.

DELIVERABLE 2.5 – NEMSIS COMPLIANT DATA FROM EMS PROVIDER AGENCIES

COUNTY shall be able to validate the NEMSIS compliant data from EMS provider agencies are successfully imported into the EMS Repository through the NEMSIS website.

SUBTASK 2.6 – DEVELOP NEMSIS EXPORT

The EMS Repository shall allow County to create file exports from the EMS Repository that are compliant with latest NEMSIS Standards.

DELIVERABLE 2.6 – NEMSIS EXPORT

COUNTY shall be able to validate that NEMSIS compliant data from the EMS Repository was successfully submitted to CEMSIS.

SUBTASK 2.7 – IMPLEMENTATION OF ESO'S INSIGHT REPORTING PLATFORM

CONTRACTOR shall deliver and provide the COUNTY access to ESO's Insight Reporting Platform for report generation of data residing in the EMS Repository.

DELIVERABLE 2.7 – ACCESS TO ESO'S INSIGHT REPORTING PLATFORM

CONTRACTOR shall provide the COUNTY written certification verifying access to ESO's Insight Reporting Platform and COUNTY is able to generate reports from the EMS Repository.

TASK 3 – CONDUCT ACCEPTANCE TEST FOR EMS REPOSITORY

The Build and Implementation of the EMS Repository shall not achieve Acceptance by the COUNTY unless and until all of the following have occurred:

3.1 CONTRACTOR has successfully completed Task 2 – Build and Implement the EMS Repository as set forth in this Statement of Work and each and every Deliverable thereunder has been delivered to the COUNTY and has been approved in writing by COUNTY's Project Manager.

3.2 EMS Repository meets all technical requirements and specifications in accordance with Attachment A.2 – EMS Repository Technical Requirements and Specifications, and all functional requirements in accordance with Attachment K – EMS Repository Functional Requirements.

3.3 CONTRACTOR has successfully completed all the Acceptance Tests set forth in Attachment C.2 – Acceptance Test for the EMS Repository.

DELIVERABLE 3 – ACCEPTANCE TEST FOR EMS REPOSITORY

CONTRACTOR shall conduct all the Acceptance Tests set forth in Attachment C.2 – Acceptance Test for the EMS Repository and Attachment K – EMS Repository Functional Requirements, and accepted by COUNTY's Project Manager to have successfully met the Acceptance Test Criteria.

TASK 4 – MAINTAIN LEGACY DATA FROM FIRE RESCUE

CONTRACTOR shall archive data residing in the legacy Fire Rescue One data registry, at minimum, ten (10) years of legacy data; and provide a mechanism for COUNTY to abstract and report on these legacy data. Such data shall not be commingled with NEMSIS data.

DELIVERABLE 4 – DATA RESIDING IN FIRE RESCUE

CONTRACTOR shall certify in writing that the legacy data residing in Fire Rescue One are archived to a platform that would allow reporting of these legacy data and provide COUNTY secure access and a process to abstract and report all archived data.

TASK 5 - TRAINING

CONTRACTOR shall provide the following training, in each case provided by suitably qualified and experienced trainers:

5.1. When not specified herein, CONTRACTOR's Project Manager and COUNTY's Project Manager shall jointly determine maximum class size appropriate for each training session level and the number of training sessions offered.

5.2. Orientation Training – up to 4 hours – Provide training to equip COUNTY team with understanding on context of the decisions required in configuration – building block and how they affect decisions made.

5.3. System Administration Training – up to 8 hours for up to 10 COUNTY users – Training will include training in the administration of the software, user security roles and system access.

5.4. Pre-User Acceptance Test (UAT) Training – up to 8 hours – Training sessions led by CONTRACTOR to help COUNTY UAT staff understand navigation and terminology to conceptualize the system/processes prior to Train-the-Trainer. This training may be combined with other training events, and delivered on-line/remotely.

5.5. Train-the-Trainer Training – up to 16 hours – CONTRACTOR shall provide Super User training for COUNTY staff prior to Go-Live as part of one combined training class. This training, prior to Go-Live, will be instructor led. The objective is to include training of all Super Users on all EMS Repository modules and support maintenance functions. Training plan will require approval of COUNTY's Project Manager. A training session will be led by one CONTRACTOR Trainer on-site for up to ten (10) COUNTY participants and on-line (remote) for up to twenty (20) COUNTY participants.

5.6. Post Go-Live Training – up to 20 hours

CONTRACTOR shall provide post-implementation training – 20 hours of on-line training (training type of either System Administrator, Technician or IT support to be determined by COUNTY's Project Manager). This will be to provide refresher trainings on all EMS Repository aspects and functionalities, as needed by COUNTY. This training will be delivered during a period between 6 weeks and 6 months following Go-Live.

DELIVERABLE 5 – TRAINING

CONTRACTOR shall provide COUNTY training and training materials as required under Task 5.

TASK 6 – DEPLOY TO PRODUCTION: GO-LIVE

6.1 Upon completion of User Acceptance Testing by COUNTY, CONTRACTOR shall copy the configuration into the Production Environment. CONTRACTOR

shall analyze the configured EMS Repository to ensure that it meets COUNTY's specifications. CONTRACTOR's activities under this Task shall include, at a minimum:

1. Resolving issues identified during UAT testing cycles.

2. Training COUNTY System Administrators in the administration of the SaaS platform.

3. Generating Production Checklist outlining all cutover activities with completion dates, times and owner for each task.

4. Performing required Go-Live and post Go-Live configuration activities that are assigned to Contractor, including technical and business support.

5. Designating an Implementation Consultant who shall provide remote Go-Live support as agreed to by the parties.

6.2 The SaaS platform shall be deemed fully functional and ready for live and operational use ("Go-Live") upon successful completion of the UAT and when all discovered during the UAT (i) material deficiencies and (ii) any other issues which COUNTY considers critical or which are not scheduled to be resolved in an upcoming software release have been resolved, unless COUNTY agrees in writing for any such non-material issues to be resolved following Go-Live.

DELIVERABLE 6 – CUTOVER TO PRODUCTION: GO-LIVE

6.1 CONTRACTOR shall develop a Cutover Plan which shall all track activities during the cutover from the current Legacy System to the new SaaS Platform.

6.2 CONTRACTOR shall develop a Production Checklist of all COUNTY activities required for successful Go-Live of the EMS Repository in the Production Environment.

TASK 7 – PROVIDE POST GO-LIVE SUPPORT

CONTRACTOR shall provide post Go-Live Support. CONTRACTOR's activities under this Task shall, at a minimum, include:

Providing Post Go-Live Support to assistance rollout, including post Go-Live remote support, refresher training and/or general questions. In the event critical or material EMS Repository issues are discovered during the Post Go-Live Support Period (e.g., with Critical Business Impact, Service Down or Significant Business Impact), CONTRACTOR's staff shall provide support until the resolution of all such issues is mapped out and agreed to by COUNTY's Project Manager, at no additional cost to COUNTY.

DELIVERABLE 7 – POST GO-LIVE SUPPORT

CONTRACTOR shall assemble and provide to COUNTY appropriate deliverable documentation for the Software.

3 ATTACHMENT A.2 – EMS REPOSITORY TECHNICAL REQUIREMENTS AND SPECIFICATIONS

3.1. GENERAL TECHNICAL REQUIREMENTS

3.1.A. EMS REPOSITORY ADMINISTRATION

1. The EMS Repository shall allow authorized site-specific users to manage site-specific user groups and user accounts, up to and including their level of authority.

2. The EMS Repository shall allow all users to reset their own passwords.

3. The EMS Repository shall allow administrators to delegate authority, by user group to restore EMS Repository access of locked out user.

4. The EMS Repository shall provide the ability to restrict access based on user's account privileges.

5. The EMS Repository shall provide the ability to specify roles and privileges based on IP locations.

6. The EMS Repository shall allow the restriction of rights, privileges or access by user or security role.

7. The EMS Repository shall allow restricting the rights, privileges, or access of processes to the minimum required for authorized tasks.

8. The EMS Repository shall have the ability to display the last date and time the user logged onto the EMS Repository at the time of logon.

9. The EMS Repository allows revocation of the access privileges of a user without requiring deletion of the user.

10. They EMS Repository shall allow assigning multiple roles to one user.

3.1.B. ADMINISTRATIVE REPORTING

1. The EMS Repository shall implement event, audit and access logging that complies with current HIPAA Security Rule.

2. The EMS Repository shall provide summarized and detailed reports on COUNTY user access, and other standard back-end administrative reporting.

3. The EMS Repository shall provide online reporting capability to authorized County System managers for necessary review and accountability.

4. The EMS Repository shall allow Contractor to respond to periodic requests for:

   - Configuration, user accounts, roles and privileges reports.

- Listing of privileged account holders within the EMS Repository environment.

3.1.C. CONFIGURATION MANAGEMENT

1. The EMS Repository shall provide the ability to maintain multiple operating environments for development, test, training, and production.

2. The EMS Repository shall ensure administration interfaces require strong authentication and authorization.

3. The EMS Repository shall provide administrator privileges that are separated based on roles (e.g., site content developer, System administrator).

4. The EMS Repository shall provide secured remote administration channels (e.g., SSL, VPN).

5. The EMS Repository shall provide configuration stores that are secured from unauthorized access and tampering.

6. The EMS Repository shall provide configuration credentials and authentication tokens held in plain text in configuration files (e.g., client configuration file with remote ID login and password).

7. The EMS Repository shall provide user accounts and service accounts used for configuration management that provide only the minimum privileges required for the task.

3.2. EMS REPOSITORY SECURITY REQUIREMENTS

3.2.A. USER PROFILES/ROLES

1. The EMS Repository shall provide the ability for users to define and store user profile information, including but not limited to, the user's name, user ID, employee ID, professional designation, etc.

2. The EMS Repository shall have the ability to link the user logon ID to his/her employee number, as well as to the location or group of locations to which the user is assigned.

3. The EMS Repository shall provide the ability to define user roles and user groups and associate these with user accounts.

4. The EMS Repository shall allow the creation and assignment of user roles that limit a user's privileges to their scope of practice.

5. The EMS Repository shall have role-based security and shall enable access of reports and dashboards to be restricted to specific roles based on security levels.

6. The EMS Repository shall allow the creation and assignment of user roles that define their required and allowed actions in workflows.

7. The EMS Repository shall allow the assignment of multiple roles to be selected from the user at login.

8. The EMS Repository shall allow users to customize their interfaces with favorited or regularly used reports.

3.2.B. EMS REPOSITORY ACCESS

1. The EMS Repository shall provide ability to use a single user sign-in for all modules with security configured for each module.

2. The EMS Repository shall have the ability for secure module to be maintained by an in-house System Administrator as to COUNTY employees.

3. The EMS Repository shall allow an unlimited number of users to access and use the EMS Repository at the same time.

4. The EMS Repository shall automatically notify users and force them to change passwords on a pre-defined frequency.

5. The EMS Repository shall provide an efficient, flexible way to control and administer multiple levels of user access.

6. The EMS Repository shall have the ability to support web-based client access or other internet-based client access technologies, with appropriate security access controls.

7. The EMS Repository shall provide password complexity EMS Repository standards.

8. The EMS Repository shall provide the password change rules for user accounts.

9. The EMS Repository shall provide lock-out capability after a pre-defined number of unsuccessful user sign-on attempts.

10. The EMS Repository shall not display passwords as clear text (Password Masking).

11. The EMS Repository shall provide integrated security managed in a central accounts database.

12. The EMS Repository shall encrypt passwords before being stored or transmitted.

13. The EMS Repository shall allow users to re-authenticate and remotely log out of an active user session before logging in at another location.

14. The EMS Repository shall encrypt sensitive data transmitted between clients and serves using Secure Socket Layer (SSL) Certificates, Transport Layer Security (TLS), or by other means.

15. The EMS Repository shall restrict users, based on their security rile from directly accessing the database.

16. The EMS Repository shall allow secure password resets in case passwords are forgotten.

17. They EMS Repository shall have the ability to assign application access rights across entire suite of applications at a single point of entry.

18. The EMS Repository shall support a pre-defined time for passwords to be changed and suspended per user's role, access level and defined inactivity period. The COUNTY standard for users in 90 days.

3.2.C. AUTHENTICATION

1. The EMS Repository shall ensure all EMS Repository and user accounts are identified.

2. The EMS Repository shall ensure Multi-Factor authentication for public facing access to the application.

3. The EMS Repository shall ensure web sites are partitioned into un-restricted and restricted areas using separate folders.

4. The EMS Repository shall provide authentication that users least-privileged accounts.

5. The EMS Repository shall ensure that minimum information is returned in the event of authentication failure.

6. The EMS Repository shall ensure credentials are secured/encrypted in storage, and over the wire via Secure Socket Layer (SSL/TLS 1.2 or higher) or IP Security (IPSec), if Structured Query Language (SQL) authentication is used (e.g., communication between the application server and the database server).

3.2.D. AUTHORIZATION

1. The EMS Repository shall ensure measures are in place to prevent, detect and log unauthorized attempts to access the EMS Repository.

2. The EMS Repository shall ensure rights and privileges are assigned based on authorization roles.

3. The EMS Repository shall ensure database restricts access to stored procedures to authorized accounts only.

4. The EMS Repository shall ensure all account IDs that are used by the EMS Repository are identified and the resources accessed by each account is known.

5. The EMS Repository shall ensure roles are mapped to user and data interfaces. Role rights and privileges are identified and maintained in an access control list.

6. The EMS Repository shall ensure resources are mapped to EMS Repository roles and allowed operations for each role.

3.2.E. INTEGRITY CONTROLS

1. The EMS Repository shall ensure measures are in place to detect unauthorized changes to information.

2. The EMS Repository shall ensure measures are in place to protect information from being accidentally overwritten.

3. The EMS Repository shall support integrity mechanisms for transmission of both incoming and outgoing files, such as parity checks and cyclic redundancy checks. (CRCs).

4. The EMS Repository shall ensure measures are in place to prevent the upload of unauthorized files (e.g., executable files).

3.2.F. SENSITIVE DATA (E.G., EPHI, PERSONALLY IDENTIFIABLE INFORMATION)

1. The EMS Repository shall ensure sensitive data and secrets are not incorporated in code.

2. The EMS Repository shall ensure secrets are stored securely using a one-way hash. Database keys, connections, passwords, or other secrets are not stored in plain text.

3. The EMS Repository shall ensure sensitive data is not logged in clear text by the EMS Repository.

4. The EMS Repository shall ensure sensitive data is not transmitted using insecure protocols, such as FTP, telnet, sftp, etc., unless through an authenticated encrypted connection (e.g., VPN).

5. The EMS Repository shall ensure sensitive data is not sorted in persistent cookies.

6. The EMS Repository shall ensure measures are in place to prevent, detect and log unauthorized attempts to access sensitive or confidential data.

7. The EMS Repository shall restrict transactions involving financial or sensitive data to authorized user sessions originating on the County Intranet WAN only. Access to such transactions from the Internet is blocked.

8. The EMS Repository shall restrict access to financial transactions and other sensitive data by authorized users outside the County Intranet to Read Only mode.

9. The EMS Repository shall ensure all user sessions involving financial transaction or sensitive data are encrypted using SSL/TLS 1.2 or higher/HTTPS.

10. The EMS Repository shall provide administrative ability to block user's access to individual patient records for privacy reasons.

3.2.G. ENCRYPTION

1. The EMS Repository shall have the ability to encrypt electronic PHI at rest or in motion, and support all required encryption process, to conform with the current HIPAA Security Rule.

3.2.H. INPUT VALIDATION

1. The EMS Repository shall ensure that input validation is applied whenever input is received through user or external data interfaces. The validation approach is to constrain, reject, and then sanitize input.

2. The EMS Repository shall be designed with EMS Repository validation that assumes that user input is malicious.

3. The EMS Repository shall validate data from type, length, format, and range. Data validation is consistent across the EMS Repository.

4. The EMS Repository shall be designed to avoid un-trusted input of file name and file paths. (i.e., does not accept file names or file paths from calling functions. Decisions are not made based on user-supplied file names or paths.)

5. The EMS Repository shall be designed so that the EMS Repository does not use parent paths when data within the EMS Repository is being accessed. Attempts to access resources using parent paths are blocked.

6. The EMS Repository shall ensure web server always asserts a character set: a locale and county code.

3.2.I. TIMEOUTS

1. The EMS Repository shall provide an automatic timeout if the session is idle for a prespecified and configurable duration.

2. The EMS Repository shall warn the user before the timeout and prompts the user to re-enter their password.

3.2.J. PARAMETER MANIPULATION

1. The EMS Repository shall ensure all input parameters are validated (including form fields, query strings, cookies, and HTTP headers).

2. The EMS Repository shall support cookies with sensitive data (e.g., authentication cookies) are encrypted,

3. The EMS Repository shall ensure sensitive data is not passed in query strings of form fields.

4. The EMS Repository shall support security decisions on information other than HTTP header information.

3.3. SYSTEM USE AND INTEROPERABILITY

3.3.A. SCALABILITY

1. The EMS Repository shall be scalable and adaptable to meet any reasonable future growth and expansion needs.

2. The EMS Repository shall contain a single database for all solutions and modules.

3.3.B. INTERFACES

1. The EMS Repository shall support standard Application Programming Interface (API).

2. The EMS Repository shall support standard Simple Object Access Protocol.

3. The EMS Repository shall provide the ability to validate incoming messages.

4. The EMS Repository shall provide the ability to perform data transformations.

5. The EMS Repository shall provide the ability to load information from NEMSIS-standard XML.

6. The EMS Repository shall be scriptable/programmable using an industry standard language.

7. The EMS Repository shall support standard logging levels (WARN, INFO, DEBUG, TRACE) at the interface layer.

8. The EMS Repository shall have the ability to evaluate interface messages for accuracy, completeness, and reject messages that are not constructed properly as well as the capability to generate reports of failed messages.

9. The EMS Repository shall have the capability to analyze, correct and resend messages that have been rejected.

3.3.C. The EMS Repository shall provide the ability to automatically transfer data to external agencies on a real-time (or near real-time) basis.

3.3.D. DATA CONVERSION

1. The CONTRACTOR shall provide all services needed to transform, standardize, migrate, and load external legacy electronic data in order to establish an initial database suitable for life organization operations.

3.3.E. FLEXIBILITY

1. The EMS Repository shall ensure functionality and associated business rules shall be configurable without requiring “code” modifications.

   The EMS Repository shall provide screens that reflect the data fields/elements that are selected by County.

2. The EMS Repository shall provide the ability to create and/or modify the business rules which determine the acceptance/correctness of data.

3. The EMS Repository shall provide the ability for on-line access by any site connected to the organization WAN.

4. The EMS Repository shall provide the ability for secure remote access by authorized individuals (e.g., web-based VPN access).

3.3.F. END-USER INTERFACE

1. The EMS Repository shall use the standard out-of-the-box GUI tools to create solution user interfaces.

2. The EMS Repository shall ensure that all components are substantially compliant with the American Disabilities Act (ADA) and Section 508.

3. The EMS Repository shall provide dynamic content and views based on user role.

4. The EMS Repository shall have a customizable online documentation and training materials such as context-specific help, search capability, organization-specific business process documentation and process maps.

5. The EMS Repository shall provide the ability for a single user to open multiple sessions concurrently.

3.3.G. REPORTING

1. The EMS Repository shall present data in graphical (e.g., charts, graphs) and numeric displays based on data with the EMS Repository.

2. The EMS Repository shall have the ability to export reports directly to Excel, HTML, or PDF formats.

3. The EMS Repository shall provide ad hoc and standard query capabilities (with and without input parameters).

4. The EMS Repository ad hoc reporting tool shall be able to access any delivered or added filed in the database.

5. The EMS Repository shall provide ability to create and maintain a report distribution mechanism with predefined reports (e.g., monthly reports that are specific by role, organization, and location via portal or Web).

6. The EMS Repository shall provide security to protect reports created by one user from being viewed, modified, and /or executed by another user.

7. The EMS Repository shall provide the ability to view the fields selected for previously generated reports by any user, provided that the data in such fields for the report are not stored when generated.

8. The EMS Repository shall provide capability to schedule reports and dashboards to run automatically according to County specified intervals.

9. The EMS Repository shall allow for reporting by exception.

10. The EMS Repository shall allow print preview of all reports before printing and have print screen and selective page(s) print functionality.

11. The EMS Repository shall allow for user-friendly end-use report creation without requiring technical staff or expertise to create and publish reports within the modules.

3.3.H. CONTENT AND DOCUMENT MANAGEMENT

1. The EMS Repository shall have the ability to scan, attach and store imaged (scanned) documents and electronic files.

2. The EMS Repository shall enable indexing and searching of documents by a variety of user-define metadata attributes.

3. The EMS Repository shall support for full text search.

4. The EMS Repository shall enable attachment of documents to e-mails and e-mail distribution lists.

3.4. HOSTING REQUIREMENTS

3.4.A. HOSTING SERVICE OVERVIEW

1. The CONTRACTOR's hosting services is permitted to be provided by Microsoft's Azure (commercial) services, and subject to its features and availability. CONTRACTOR shall be responsible for using Azure as its hosting provider.

2. The CONTRACTOR's hosting services shall provide adequate firewall protection in order to secure Personal Data and other Confidential Information users of the EMS Repository from unauthorized access by third parties.

3.4.B. CLOUD HOSTING

1. The EMS Repository shall be hosted on an industry standard cloud hosting platform.

2. The CONTRACTOR's hosting services cloud solution must allow for hosting in the cloud without excessive effort and/or re-configuration.

3.4.C. HOSTING SERVICE OPERATIONS

1. The CONTRACTOR shall have a process in place for transitioning from development to production operations.

2. The CONTRACTOR shall have well established maintenance and management procedures.

3. The CONTRACTOR shall have a documented process for capacity planning and management.

4. The CONTRACTOR shall have a documented methodology for monitoring, measuring, and reporting the performance metrics and EMS Repository accounting information.

5. The CONTRACTOR shall have a documented procedure for management of staff and operations 24 hours per day, 7 days per week, and 365 days per year.

6. The CONTRACTOR shall monitor computing systems and communications circuits 24 hours per day, 7 days per week, 365 days per year.

7. The CONTRACTOR shall have a documented procedure for incident response and escalation.

8. The contractor shall maintain an industry standard, ITIL-based Change Management process and system.

9. The CONTRACTOR shall have a documented procedure for managing, monitoring, and maintaining interfaces.

10. The CONTRACTOR shall manage and clearly communicate roles and responsibilities for its staff and COUNTY staff.

11. The CONTRACTOR shall provide continuous monitoring and management of the Hosting Environment to optimize support, performance, and EMS Repository availability.

12. The CONTRACTOR shall provide a means for the COUNTY to monitor EMS Repository uptime and response time of the Hosted Services.

13. The CONTRACTOR shall provide and maintain a method for escalation of issues, and log all incidents, problems and error corrections.

3.4.D. HOSTING SERVICE DISASTER PREPAREDNESS & RECOVERY

1. The CONTRACTOR shall have a documented procedure for responding to unscheduled downtime.

2. The EMS Repository shall meet a Recovery Time Objective (RTO) of 24 hours and Recovery Point Objective (RPO) of 24 hours.

3. The CONTRACTOR shall have documented strategy, architecture and procedures for Business Continuity that meet industry standards for RTO of 24 hours and RPO of 24 hours.

4. The CONTRACTOR shall have a documented strategy, architecture and procedures for Disaster Recovery that meet industry standards for RTO of 24 hours and RPO of 24 hours.

5. The CONTRACTOR shall have a documented strategy, architecture, and procedures for Backup/Restore that meet industry standards for RTO of 24 hours and RPO of 24 hours.

6. The CONTRACTOR shall have a documented procedure for prompt client communication in the event of an unscheduled downtime.

7. The EMS Repository shall have the ability to seamlessly failover to a secondary site in a different geographic location and/or disaster zone.

8. The EMS Repository shall have the ability to report on uptime/downtime history.

3.4.E. HOSTING SERVICE SECURITY

1. The CONTRACTOR shall be responsible for physical and logical security for all service components (hardware and software) and data.

2. The CONTRACTOR shall complete DHS SaaS questionnaire and provide their SOC2 Type II report with a corrective action plan for any identified weaknesses.

3. The CONTRACTOR shall use industry standard encryption for all data at rest or in motion.

4. The CONTRACTOR shall provide intrusion detection and prevention, including network intrusion and virus detection systems throughout Hosted Services network and computing infrastructure.

5. The CONTRACTOR shall meet the requirements of the current federal HHS HIPAA Security Rule.

3.4.F. HOSTING SERVICE LEVELS

1. The CONTRACTOR shall provide an approach for defining and calculating System availability.

2. The EMS Repository shall maintain 99.5% availability for the SaaS Platform for webservice submissions from agencies and for COUNTY application access, excluding planned maintenance.

3. The CONTRACTOR shall respond to reasonable inquiries regarding Service Level performance and monitoring activities.

4 ATTACHMENT B.2 – SUPPORT SERVICES, MAINTENANCE SERVICES, AND SERVICE LEVELS FOR EMS REPOSITORY (SAAS PLATFORM)

4.1 SUPPORT SERVICES

Support services shall include all goods and services necessary to manage, operate and support the SaaS Platform to comply with the requirements and specifications. Support services, include, but are not limited to, help-desk support during support hours and off-hours, , regular updates and/or patches required to fix defects or issues, and access to knowledgeable CONTRACTOR personnel who can answer questions on the use of the SaaS Platform or provide analysis on SaaS Platforms to operational problems.

The support services shall be in accordance with Contractor's standard SaaS support terms attached hereto as Attachment L, and include:

A. Software updates to the SaaS Platform to keep current with industry standards, enhancements, updates, patches, bug fixes, etc., the specifications, the requirements and as provided to CONTRACTOR general customer base, in coordination with COUNTY Project Manager. Software updates shall include, but not be limited to, enhancements, version releases and other improvements and modifications to the SaaS Platform. Without limiting any other provisions of the Agreement, including, without limitation, the statement of work, software updates to the SaaS Platform shall be provided to COUNTY at least every year, unless otherwise agreed to by COUNTY and CONTRACTOR.

1. CONTRACTOR shall notify COUNTY of all software updates to the SaaS Platform prior to the anticipated installation date thereof. CONTRACTOR provision and installation of such software updates to the SaaS Platform shall be at no additional cost to COUNTY beyond any applicable support fees. Any software updates necessary to remedy security problems in the SaaS Platform (e.g., closing "back doors" or other intrusion-related problems) shall be provided promptly following CONTRACTOR knowledge of such problems. COUNTY shall also be notified in writing within five (5) calendar days of CONTRACTOR knowledge of the existence of any intrusions or other security problems or breaches that materially affect the integrity of the SaaS Platform.

2. CONTRACTOR shall correct any failure of the SaaS Platform and deliverables to perform in accordance with the requirements, including without limitation, defect repair, programming corrections, and remedial programming, and provide such services and repairs required to maintain the SaaS Platform and deliverables so that they operate properly and in accordance with the requirements.

B. Maintenance of the SaaS Platform's compatibility with TEMIS Facilities (Attachment C) Environment by providing, among others, software updates to the SaaS Platform and hardware upgrades to the SaaS Platform hardware.

C. Help desk support including access to knowledgeable CONTRACTOR personnel who can answer questions on the use of the SaaS Platform or provide analysis on SaaS Platforms to operational problems, which TEMIS Facilities may encounter during support hours. The CONTRACTOR help desk support shall be made available to the COUNTY from 6 A.M. Pacific Standard Time to 6 P.M. Pacific Standard Time. Including unlimited telephone access to help desk support. The CONTRACTOR shall answer calls received by the answering service based on the criticality of the request as described below.

D. Online access technical support bulletins and other user and self-help support information and forums.

E. Support Requests

CONTRACTOR shall respond to COUNTY support service requests as part of support services. CONTRACTOR shall:

1. Set up a service request tracking SaaS Platform as required below.

2. Participate in weekly meetings with COUNTY to discuss status of, and improvement of response time to, service requests.

3. Provide recommendations to COUNTY for issue identification and resolution procedures, including steps to diagnose whether issues originate in COUNTY-owned or TEMIS Facility-owned or CONTRACTOR-controlled settings.

4. Notify COUNTY of any issues CONTRACTOR discovers that materially and adversely impact the SaaS Platform.

5. Provide, manage, and maintain a method for proper notification and escalation of issues.

6. Log all incidents and problems.

7. Provide incident and management reports and statistics to COUNTY as requested by COUNTY.

8. Conduct calls as requested by COUNTY to discuss service requests and related issues.

9. Report monthly on service requests, including the tracking and reporting of any issues.

CONTRACTOR shall not withhold support services due to any dispute arising under the Agreement, another Agreement between the parties, or any other related or unrelated dispute between the parties. CONTRACTOR shall not remove from COUNTY facilities or retain a copy of any COUNTY data obtained from, or as a result of access to, COUNTY systems unless

that removal or retention is reasonably necessary to perform the support services or is otherwise approved in writing by COUNTY.

F. CONTRACTOR's customer support shall also include:

1. COUNTY and TEMIS Facilities designated technical support staff that provide first level support shall have access to CONTRACTOR's customer support through the methods outlined in this Attachment.
2. CONTRACTOR shall provide a telephone number for COUNTY and TEMIS Facilities staff to call during normal business hours. This telephone number shall be managed by an automated system to quickly connect COUNTY and TEMIS Facilities staff with the appropriate customer support personnel.
3. CONTRACTOR's automated system shall include the functionality of leaving detailed voice mails describing the issues. The voice mails and live support must be responded to based on the criticality of the request (see Section 4.4.A Support Request Service Levels).
4. CONTRACTOR's customer support shall made be available to COUNTY during the hours of 6 A.M. Pacific Standard Time to 6 P.M. Pacific Standard Time.

G. Service Request Tracking System

1. For use in responding to COUNTY's maintenance and support requests, CONTRACTOR shall maintain an automated Support Request Tracking System ("SRTS") with a description of each support request, response, and status. CONTRACTOR shall review and update all open support requests and follow up on unresolved support requests on a weekly basis. CONTRACTOR will provide COUNTY "read only" access to the SRTS for COUNTY's separate review of all open and closed COUNTY support requests. Each support request shall be detailed in an internet accessible support request report, in an exportable format agreed upon by COUNTY, and shall include the following information.

    a. Identification Number. An automatically assigned unique identification number, which shall be used to track, document and respond to inquiries relating to a specific support request.

    b. Date and Time. The date and time the support request was initiated, which shall be used to document and/or monitor overall response and resolution time.

    c. Support Contact: The name, title, and telephone number of the person initiating the support request, who shall be the primary point(s) of contact used for inquiries regarding the request, unless otherwise assigned by COUNTY's Project Manager.

d. Call Taker. The name of CONTRACTOR personnel taking the call or first receiving an electronically submitted support request.

e. CONTRACTOR employee currently assigned. The name and title of the CONTRACTOR's employee currently managing the resolution.

f. Error Correction. Means (i) with respect to the SaaS Platform, either a modification to the SaaS Platform that corrects an error in all material respects, or a procedure or routine that, when implemented in the regular operation of that SaaS Platform, eliminates the adverse effect of the error in all material respects, and (ii) with respect to services or deliverables, modification, workaround, or performance that corrects an error in all material respects or eliminates the adverse effects of the error in all material respects.

g. Location. Facility and/or physical location where the problem occurred.

h. Error Priority Level. The error priority level as indicated in Attachment L.

i. Reference Number. The COUNTY-assigned reference number, if applicable.

j. Service Request Description. A detailed description of the problem or error encountered or support requested.

k. Attached Documentation. The identification or description of, and, if available, copies of, documentation submitted by COUNTY with the support request to clarify the request, including screen prints, logs, report samples, etc.

l. Service Request Type. The support request type (e.g., software change, error, report request, etc.), as assigned by COUNTY which categorizes and specifies the type of request.

m. Service Request Subtype. The support request subtype (e.g., specific function to be changed, specific function that is deficient, type of report change requested, etc.), as assigned by COUNTY, as a subcategory of the service request type defined in Section 4.4.A. (Support Request Service Levels) of this Attachment.

n. Resolution Description. The CONTRACTOR's analysis of the problem, and the proposed resolution (e.g., revision).

o. Resolution Platform Activity. The CONTRACTOR's resolution activities and activity dates to monitor resolution time (e.g., description of calls to and from CONTRACTOR and

COUNTY, referrals to CONTRACTOR's staff for correction or investigation, referrals to third party product vendor, coordination of revision releases, validation of correction prior to release to COUNTY, etc.).

p. Estimated Fix Date. The estimated date for CONTRACTOR to complete the support request.

q. Correction Applied Date. The date CONTRACTOR applied the correction.

r. Resolution Status. The current status of the support request (e.g., open or closed).

2. CONTRACTOR shall maintain a historical knowledge base of support service-related problems to identify patterns and facilitate timely resolution.

4.2 MAINTENANCE SERVICES

Maintenance Services shall include all goods and services necessary to provide and maintain the back-end of the SaaS Platform in order to comply with the requirements and specifications. The Maintenance Services shall be considered part of the provision of the SaaS Platform and shall be provided to at no additional cost to COUNTY beyond the applicable fees for the SaaS Platform.

As part of Maintenance Services, CONTRACTOR shall provide maintenance of the server software that is part of the server environment ("Server Environment") for the SaaS Platform, including but not limited to operating software, database software and other software installed in the Server Environment that is not licensed software ("Server Software"). CONTRACTOR shall update, upgrade or replace these server software components during the Term of the Agreement to comply with the specifications, the requirements and the warranties specified in the Agreement and to support and be compatible with the licensed software including any revisions provided by CONTRACTOR under the Agreement.

Maintenance Services shall include:

A. SaaS Platform Hosting

Provide the SaaS Platform to COUNTY and TEMIS Facilities on a 24 hours per day, 7 days per week, 365 days per year basis in accordance with the Agreement and Attachment J (Hosting Services Terms and Conditions) of the Agreement.

B. SaaS Platform Monitoring

CONTRACTOR will perform continuous monitoring and management of the SaaS Platform to optimize availability of the SaaS Platform. Included within the scope of this sub-paragraph is the proactive monitoring of the server and all service components of CONTRACTOR's hosting environment and

firewall for trouble on a 7 day by 24 hour basis. CONTRACTOR shall maintain redundancy in all key components such that outages are less likely to occur due to individual component failures. CONTRACTOR will monitor "heartbeat" signals of all servers, routers, and leased lines, and http availability of the SaaS Platform, by proactive probing at 30-second intervals 24 hours a day using an automated tool. If a facility does not respond to a ping-like stimulus, it shall be immediately checked again. When CONTRACTOR receives a "down" signal, or otherwise has knowledge of an outage or error (including, without limitation, any failure in the server or application software and/or hardware used to provide the SaaS Platform), CONTRACTOR personnel will:

1. Confirm (or disconfirm) the Outage by a direct check of the facility.

2. If confirmed, take such action as may restore the service, or, if determined to be an internet service provider or telecom carrier problem, open a trouble ticket with the relevant companies.

3. Notify COUNTY by telephone according to mutually agreed upon procedures if an outage is expected to last more than two hours.

4. Work each error until resolution, escalating to management or to engineering as required.

4.3 BACKUPS

CONTRACTOR shall provide for both the regular back-up of standard file systems relating to the SaaS Platform and COUNTY data, and the timely restoration of such data on request by COUNTY due to a SaaS Platform failure. All COUNTY systems that need to be taken offline need either a request for change or a standard operating procedure in place before they are taken offline. in particular, CONTRACTOR shall:

A. Perform weekly full back-ups.

B. Perform daily incremental back-ups.

C. Retain one back-up of the SaaS Platform's transactional database per month for 35 days.

D. Fulfill restoration requests as directed by COUNTY due to site failures. Restoration will be performed in accordance with Azure service levels.

E. Periodically review and validate CONTRACTOR's backup procedures, and periodically validate the accuracy and integrity of the backup data. CONTRACTOR shall provide a written report of any inaccuracies and inconsistencies in a format approved by COUNTY.

4.4 SERVICE LEVELS

A. Support Request Service Levels

CONTRACTOR shall respond to and Resolve Support Requests as set forth in this Attachment B.2.

1. Escalation. With respect to any Critical Support Request, until Resolved, CONTRACTOR shall escalate that Support Request within sixty (60) minutes or as quickly as reasonably practicable of Receipt to the appropriate CONTRACTOR support personnel (as designated by CONTRACTOR), including, as applicable, CONTRACTOR's Supervisor of Client Operations.

B. Availability Service Level

The SaaS Platform shall be available for the percentage of the time each month of the term of the Agreement as set forth below:

In each calendar month of the term of the Agreement, the SaaS Platform shall maintain 99.5% availability for webservice submissions from agencies and for COUNTY application access, in each case excluding planned maintenance.

"Availability" means the actual uptime expressed as a percentage of the scheduled uptime for the SaaS Platform (i.e., availability % = ((scheduled uptime – downtime)/(scheduled uptime)) × 100%).

"Scheduled Uptime" means twenty-four (24) hours each day, seven (7) days per week, excluding regular maintenance windows following notification to the COUNTY. Notwithstanding anything herein, CONTRACTOR shall ensure that the SaaS Platform remain available for use during the foregoing maintenance windows to the extent reasonably practicable and that maintenance shall not occur during a high-need period.

"Downtime" means the aggregate duration of outages for the SaaS Platform during the applicable scheduled uptime during a calendar month.

"Outage" means any time during which the SaaS Platform (or any portion thereof) is not available for use during a calendar month, measured from the earliest point in time that such outage is or reasonably should be detected by CONTRACTOR, but in any event no later than the time the outage actually occurred. An outage is an Error.

"Unplanned Downtime" shall mean an outage that is not the result of a regularly scheduled or other scheduled maintenance window.

"Available For Use" shall mean the ability of the SaaS Platform to be utilized or accessed by COUNTY and TEMIS Facilities as contemplated under the Agreement(s), including conformance to the requirements and specifications, and without material degradation of performance.

C. Service Level Credits

In the event 99.5% availability for the SaaS Platform for webservice submissions from agencies and for COUNTY application access is not achieved for any calendar month, then COUNTY shall receive a credit on its next annual fee invoice of 10% for each month that this level was not achieved.

D. Meetings

CONTRACTOR and COUNTY shall meet at least once every two weeks, and as mutually agreed based on caseload to review the status of open Support Requests, and discuss trends and issues relating to Support Requests and approaches to reducing the number of Support Requests as well as improving both COUNTY and CONTRACTOR responses to such Support Requests.

4.5 SERVICE LEVEL FAILURES AND SERVICE LEVEL CREDITS

A. Termination for Chronic Service Level Failures

In addition to its termination rights under the Agreement, COUNTY may, in its sole discretion, terminate the Agreement without further obligation to CONTRACTOR in the event CONTRACTOR fails to achieve the required Service Level two (2) times in any two (2) consecutive month period, or three (3) times in any five (5) month period.

4.6 CORRECTIVE ACTION PLAN

In the event two (2) or more Critical Support Requests (i.e. Severity 1 Error or Severity 2 Error) occur in any thirty (30) calendar day period during the Term of the Agreement, CONTRACTOR shall promptly investigate the root causes of such support issues and shall provide to COUNTY within five (5) business days of the occurrence of the second Critical Support Request an analysis of such root causes and a proposed corrective action plan for COUNTY's review, comment, and approval (the "Corrective Action Plan"). The Corrective Action Plan shall include, at a minimum: (a) a commitment by CONTRACTOR to devote the appropriate time, skilled CONTRACTOR personnel, systems support and equipment, and/or resources to remedy, and prevent any further occurrences of critical support request issues; and (b) time frames for implementation of the Corrective Action Plan. there shall be no additional charge (other than those fees set forth in this Agreement(s)) for CONTRACTOR's implementation of such Corrective Action Plan in the time frames and manner set forth in the Corrective Action Plan.

4.7 SERVICE OUTAGES

A. Scheduled Outages

CONTRACTOR shall notify COUNTY of Scheduled Outages at least twenty-four (24) hours in advance, and such Outages shall be scheduled between the hours of 1:00 A.M. and 5:00 A.M. Central Time on Sundays.

Scheduled Outages shall occur no more frequently than twice per calendar month. For avoidance of doubt, Scheduled Outages that fall within the above maintenance window timeframes are excluded from the availability calculation.

CONTRACTOR may request extensions of Scheduled Outages beyond the aforementioned hours and with written approval by COUNTY, which may not be unreasonably withheld, conditioned or delayed. Unscheduled Outages (as described below) and extensions of Scheduled Outages as described above are not excluded from the Availability Service Level set forth above (i.e., an outage, regardless of its cause, except due to the actions of COUNTY and its agents, shall not relieve CONTRACTOR of its obligation to achieve the Service Levels set forth herein).

B. Unscheduled Outages

Unscheduled Outages are caused by loss of connectivity to the internet, or by failure of a CONTRACTOR service. In cases where a destination is not available, or unacceptable service is reported, CONTRACTOR will attempt to determine the source of the Error and report its findings to COUNTY.

C. Corrective Action

Promptly upon notice of an outage, CONTRACTOR personnel shall:

1. Confirm (or disconfirm) the outage.
2. If confirmed, take such action as may restore the service, or, if determined to be a telecommunications company problem, open a trouble ticket with the telecommunications company carrier.
3. Notify the person designated by COUNTY by telephone or voicemail according to predefined procedures that an outage has occurred, providing such details as may be available, including the trouble ticket number if appropriate and time of outage.
4. Work the Error until Resolution, escalating to management or to engineering as required.
5. Promptly notify COUNTY of final Resolution, along with any pertinent findings or action taken.

4.8 WITHHOLDING OF SERVICES

CONTRACTOR warrants that during the Term of the Agreement it will not withhold the SaaS Platform and the support services provided hereunder, for any reason, including but not limited to a dispute between the parties arising under the Agreement, except as may be specifically authorized herein.

4.9 OEM SPECIFICATIONS

All furnished parts and work performed under the Agreement shall meet or exceed Original Equipment Manufacturer (OEM) specifications and shall meet all local, state, and federal laws, regulations and statutes governing such work.

5 ATTACHMENT C.2 – ACCEPTANCE TEST FOR THE EMS REPOSITORY

5.1. COMPLIANCE WITH TECHNICAL REQUIREMENTS

CONTRACTOR shall certify in writing that the SaaS Platform meets all the technical requirements as specified in Attachment B.2.

5.2. COUNTY ACCESS TO THE EMS REPOSITORY

This test is intended to verify successful access by COUNTY of the EMS Repository. This test will be conducted by COUNTY at the TEMIS Central Site and consists of the following steps:

1. COUNTY will attempt to access the EMS Repository via the internet. This test is successful if all COUNTY staff authorized to access the EMS Repository successfully access the EMS Repository.
2. Upon successful access by COUNTY of EMS Repository, COUNTY staff shall have access to all modules and screens based on the level authorized access.

This test will be considered successful when all authorized COUNTY staff are able to access the EMS Repository

5.3. DATA VALIDATION

This test is intended to verify successful import of NEMSIS compliant data from EMS provider agencies into the EMS Repository. This test will be conducted by COUNTY at the TEMIS Central Site and consists of the following steps:

1. COUNTY will download 10 hard copy records from the EMS Repository.
2. COUNTY will verify each data element in the EMS Repository matches the documented values in the hard copy records.

This test will be considered successful if all data elements in the EMS Repository matches the data elements in the 10 hard copy records.

5.4. REPORT GENERATION

This test is intended to verify successful report generation of standardized reports and custom reports. This test will be conducted by COUNTY at the TEMIS Central Site and consists of the following steps:

1. COUNTY will access all standardized reports. This test is successful if all standardized reports are successfully accessed by COUNTY in a preview format.

2. COUNTY will export all standardized reports directly to Excel, HTML, PDF, and XML formats. This test is successful if all standardized reports are successfully exported to Excel, HTML, PDF, and XML formats.

3. COUNTY will create 10 custom reports. This test is successful if all 10 custom reports are successfully created by County.

4. COUNTY will export all 10 custom reports directly to Excel, HTML, PDF, and XML formats. This test is successful if all 10 custom reports are successfully exported to Excel, HTML, PDF, and XML formats.

5.5. FUNCTIONAL REQUIREMENTS

This test is to verify that the SaaS platform meets all the Functional Requirements as listed in Attachment K – EMS Repository Functional Requirements. COUNTY will conduct tests to verify whether the SaaS platform meets all Functional Requirements.

This test will be considered successful if all Functional Requirements are met as listed in Attachment K – EMS Repository Functional Requirements.

6 ATTACHMENT E – LISTING OF EMS REPOSITORY PARTICIPANTS

6.1 TEMIS CENTRAL SITE

EMS Agency	10100 Pioneer Blvd, Suite 220 Santa Fe Springs, CA 90670

6.2 EMS PROVIDER AGENCIES

Name of the EMS Provider Agency	Address
Alhambra Fire Department	301 North First Street Alhambra, CA 91801
Arcadia Fire Department	710 South Santa Anita Avenue Arcadia, CA 91006
Beverly Hills Fire Department	445 North Rexford Drive Beverly Hills, CA 90210
Burbank Fire Department	311 East Orange Grove Avenue Burbank, CA 91502
Compton Fire Department	201 South Arcadia Avenue Compton, CA 90220
Culver City Fire Department	9770 Culver Boulevard Culver City, CA 90232
Downey Fire Department	11111 Brookshire Avenue Downey, CA 90241
El Segundo Fire Department	314 Main Street El Segundo, CA 90245
Glendale Fire Department	421 Oak Street Glendale, CA 91204
La Habra Heights Fire Department	1245 North Hacienda Boulevard La Habra Heights, CA 90631
La Verne Fire Department	2061 Third Street La Verne, CA 91750
Long Beach Fire Department	3205 Lakewood Boulevard Long Beach, CA 90808
Los Angeles Fire Department	200 North Main Street Los Angeles, CA 90012

Los Angeles COUNTY Fire Department	5801 South Eastern Avenue Los Angeles, CA 90040
Los Angeles COUNTY Sherriff's Department	1060 North Eastern Avenue Los Angeles, CA 90063
Manhattan Beach Fire Department	500 15th Street Manhattan Beach, CA 90266
Monrovia Fire Department	415 South Ivy Avenue Monrovia, CA 91016
Montebello Fire Department	600 North Montebello Boulevard Montebello, CA 90640
Monterey Park Fire Department	320 West Newmark Avenue Monterey Park, CA 91754
Pasadena Fire Department	215 N. Marengo Ave., Ste. 195 Pasadena, CA 91101
Redondo Beach Fire Department	401 South Broadway Street Redondo Beach, CA 90277
San Gabriel Fire Department	1303 South Del Mar Avenue San Gabriel, CA 91776
San Marino Fire Department	2200 Huntington Drive San Marino, CA 91108
Santa Fe Springs Fire Rescue	11300 Greenstone Avenue Santa Fe Springs, CA 90670
Santa Monica Fire Department	333 Olympic Drive Santa Monica, CA 90401
Sierra Madre Fire Department	232 West Sierra Madre Blvd. Sierra Madre, CA 91024
South Pasadena Fire Department	817 Mound Avenue South Pasadena, CA 91030
Torrance Fire Department	1701 Crenshaw Boulevard Torrance, CA 90501
West Covina Fire Department	1444 West Garvey Avenue West Covina, CA 91790

Name of Provider (Ambulance)	Address
American Medical Response, Los Angeles COUNTY Operations	12638 Saticoy Street South North Hollywood, CA 91605
Falck Mobile Health Corporations Dba Care Ambulance	1517 W. Braden Court Orange, CA 92868
Westmed Ambulance, Inc. Dba McCormick Ambulance Service	2020 South Central Avenue Compton, CA 90220

7 ATTACHMENT G.2 – EMS REPOSITORY IMPLEMENTATION TIMELINE

7.1 PROJECT ADMINISTRATION

CONTRACTOR shall provide project management Deliverables as specified in this Section 1 below.

DELIVERABLE NUMBER	DELIVERABLE DESCRIPTION	START DATE	END DATE
1.1	Project Work Plan	1 month upon execution of this Amendment 12	2 months upon execution of Amendment 12
1.2	Status Reports and Conferences	1 month upon execution of this Amendment 12	2 months upon execution of Amendment 12

7.2 BUILD AND IMPLEMENT EMS REPOSITORY (SAAS PLATFORM)

As part of Project Implementation, CONTRACTOR shall provide the Deliverables relating to building and implementing the EMS Repository as specified in this Section 2 below, subject in each case to the timely response and adequate resourcing of COUNTY and the applicable EMS agencies.

DELIVERABLE NUMBER	DELIVERABLE DESCRIPTION	START DATE	END DATE
2.1	Provide Hardware Specifications	1 month after execution of this Amendment 12	Within 2 months after execution of Amendment 12
2.2	Develop Schematron for EMS Repository	1 month after execution of this Amendment 12	Within 2 months after execution of Amendment 12
2.3	Provide Schematron for Publication	1 month after execution of this Amendment 12	Within 2 months after execution of Amendment 12
2.4	Develop EMS Repository that is compliant with NEMSIS 3.5 Standards	1 month after execution of this Amendment 12	Within 3 months after execution of Amendment 12
2.5	Develop NEMSIS compliant export for data submission to CEMSIS	1 month after execution of this Amendment 12	Within 3 months after execution of Amendment 12

2.6	Access to Insight Reporting Platform, Including a Test Environment	1 month after execution of this Amendment 12	Within 2 months after execution of Amendment 12
2.7	Receive and process NEMSIS compliant data from EMS provider agencies	1 month after execution of this Amendment 12	Within 3 months after execution of Amendment 12

7.3 RESERVED.

7.4 MAINTAIN LEGACY DATA FROM FIRE-RESCUE

CONTRACTOR shall provide and maintain the Deliverables relating to the Upgrade TEMIS Databases as specified in this Section IV below.

DELIVERABLE NUMBER	DELIVERABLE DESCRIPTION	START DATE	END DATE
4.1	Maintain Legacy Data from Fire-Rescue	1 month after execution of this Amendment 12	3 months after completion of activities in 7.2

8 ATTACHMENT I – BUSINESS CONTINUITY AND DISASTER RECOVERY REQUIREMENTS

This Attachment I (Business Continuity and Disaster Recovery Requirements ("BC/DR" Requirements)) is an attachment and addition to the Agreement, and is incorporated into the Agreement by reference hereof. Unless specifically defined in this Attachment, capitalized terms shall have the meanings set forth in the Agreement.

8.1 BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

CONTRACTOR shall establish, implement, and maintain business continuity, recovery, and disruption avoidance procedures for all services, including the hosting services, including hosting services provided using Subprocessors, and for the personnel and facilities providing the services, that conform with the business continuity requirements set forth throughout this Attachment I (BC/DR Requirements). CONTRACTOR shall maintain disaster avoidance procedures designed to safeguard COUNTY Confidential Information and the data processing capability, and availability of the services, throughout the Agreement Term.

In the event of an unplanned interruption of the Services, CONTRACTOR shall implement the BC/DR Plan. In an unplanned interruption of the Hosting Services, CONTRACTOR will use reasonable efforts to recover COUNTY systems and Hosting Services as quickly as possible. If CONTRACTOR fails to reinstate the Services within the periods of time set forth in the BC/DR Plan, COUNTY may in addition to any other remedies available hereunder, in its sole discretion, immediately terminate this Agreement as a non-curable default under Paragraph 30 (Termination for Default) of the Agreement.

CONTRACTOR shall promptly notify COUNTY of any disaster or other event in which the BC/DR Plan is activated with respect to COUNTY. Without limiting CONTRACTOR's obligations under this Agreement, whenever a disaster causes CONTRACTOR to allocate limited resources between or among CONTRACTOR's customers, COUNTY shall receive treatment appropriate to the nature and scope of the event with respect to such limited resources.

8.2 PLAN AUDIT

Beginning in 2024, CONTRACTOR shall have an appropriate annual audit of its BC/DR Plan, and shall provide COUNTY, upon request, with a summary of any material findings or remediation needs.

8.3 PLAN TESTING

On at least an annual basis beginning in 2024, CONTRACTOR shall actively test, review, and update the BC/DR Plan using industry standard practices as guidance, including updates to account for (i) circumstances in which interruptions to services that CONTRACTOR provides utilizing a Subprocessor prevents CONTRACTOR from delivering the services to COUNTY, and (ii) how CONTRACTOR will mitigate and restore services after such interruptions. Upon request, CONTRACTOR shall provide COUNTY with a summary of the test results and actions taken in response

to the test of the BC/DR Plan. CONTRACTOR shall provide reasonable evidence that any identified deficiencies discovered through either testing or an audit have been corrected and verified through additional testing.

8.4 REVIEW OF CONTRACTOR FACILITIES

A. Onsite Review of CONTRACTOR Facilities [omitted]

B. Review of Subprocessor Facility Compliance

As to Hosting Services provided using Subprocessors, upon request, CONTRACTOR will provide information related to the facilities used for the hosting services, including a copy of the Subprocessor's SOC report.

8.5 RECOVERY TIME REQUIREMENT

CONTRACTOR shall provide business continuity for both production use and business continuity environments according to the BC/DR Plan. In an unplanned interruption of the Hosting Services, CONTRACTOR will recover the Hosting Services as quickly as possible, and CONTRACTOR will escalate the issue to the CONTRACTOR Project Director. Working with the joint COUNTY/CONTRACTOR situation management teams, CONTRACTOR will establish an estimated time for recovery of the Hosting Services and coordinate with COUNTY to implement the most appropriate ongoing communication plan until the Hosting Services have been recovered. The CONTRACTOR Secondary Data Center or alternate Subprocessing Availability Zone, as applicable, shall be available for production use in 24 hours or less from any event in which the SaaS Platform or Hosting Services becomes unavailable, is malfunctioning, or otherwise fails to meet specifications ("Recovery Time Objective.") In addition, the CONTRACTOR Secondary Data Center or alternate Subprocessing Availability Zone, as applicable, will become available for production use with loss of data submitted by users limited to twenty-four (24) hours or less, for transactions that have not been committed to the database at the time of any failure in the SaaS Platform, licensed software or hosting services ("Recovery Point Objective").

8.6 ALTERNATE HOSTING ENVIRONMENT

A. CONTRACTOR Secondary Data Center

As to hosting services not provided using Subprocessors, CONTRACTOR will configure the hosting services to be provided from the CONTRACTOR secondary data center as described in this sub-paragraph 8.6.A (CONTRACTOR Secondary Data Center).

As of the effective date, CONTRACTOR shall have a Secondary Data Center in an alternate location deemed to be geographically dispersed. The CONTRACTOR Secondary Data Center shall not be located on the same electrical power grid or same telecommunications lines or the same: (i) floodplain, (ii) line of prevailing weather patterns, (iii) earthquake fault zone, or (iv) tsunami susceptible coastal region as the CONTRACTOR primary

data center. CONTRACTOR shall ensure the recovery site will be properly equipped with sufficient backup generators dedicated for CONTRACTOR's use to support all services, with the amount of fuel on-site that will enable the site to operate for seventy-two (72) hours or whatever the local maximum fuel storage regulations will allow. CONTRACTOR shall provide a written confirmation that it has in place written Agreements with primary and backup local fuel service providers to ensure uninterrupted replenishment of CONTRACTOR's supplies. CONTRACTOR shall provide written confirmation that its local fuel suppliers are not dependent on public commercial power in order to fulfill this requirement. CONTRACTOR is committed to continuous operation of the hosting environment including fuel for its redundant generators, however, the specific generator load capacity in the event of an outage is dependent on the conditions and cannot be specifically identified. CONTRACTOR shall ensure that the BC/DR Plan and recovery processes and procedures support relocation of hosting services performed to the recovery site to meet the requirements of this Agreement and all applicable service levels.

B. Alternate Subprocessing Availability Zone

As to Hosting Services provided using Subprocessors, CONTRACTOR will configure the Hosting Services to be provided using an alternate Subprocessing Availability Zone as described in this Sub-paragraph 8.6.B (Alternate Subprocessing Availability Zone).

As of the effective date, CONTRACTOR shall configure the Hosting Services to enable the licensed software to operate from an alternate Subprocessing Availability Zone. Subprocessing Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in facilities that are separate from the facilities used for other Subprocessing Availability Zones. The facilities used for each Subprocessing Availability Zone have a meaningful distance of separation from each other and do not share the same power infrastructure. Data center locations are managed by the Subprocessor to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. CONTRACTOR shall ensure that the BC/DR Plan and recovery processes and procedures support relocation of the Hosting Services performed to the recovery environment to meet the requirements of this Agreement and all applicable service levels.

8.7 [Omitted]

8.8 BACKUP COPIES

CONTRACTOR shall create daily backup copies of all COUNTY Confidential Information and other work related to the services and shall transmit (either electronically or via physical backup media) such copies to a backup facility each day such that the maximum data loss from the complete loss of the primary facility is no more than twenty-four (24) hours. The backup facility must be in a secured and accessible location that is geographically dispersed from the primary facility.

8.9 ALTERNATE SITES OR STORAGE FACILITIES

CONTRACTOR shall ensure that the provisions for information security, physical security, and information privacy specified in this Agreement are implemented at any alternate or backup site or storage facility and for any information transmitted between the primary site and alternate sites or storage facilities. Transport to other sites must be by secure transport carriers and any equipment for backup and/or storage must be encrypted prior to transport.

8.10 RIGHT TO TERMINATE

In the event CONTRACTOR fails to develop the foregoing recovery site and continuity practices described within this Attachment I (BC/DR Requirements) within the prescribed time, COUNTY may, in its sole discretion, terminate this Agreement without further obligation, including payment of any stranded costs.

9 ATTACHMENT J – HOSTING SERVICES TERMS AND CONDITIONS

This Attachment J (Hosting Services Terms and Conditions) is an attachment and addition to the Agreement, and is incorporated into the Agreement by reference hereof. Unless specifically defined in this Attachment, capitalized terms shall have the meanings set forth in the Agreement.

9.1 SERVICES

A. In General

CONTRACTOR shall provide and maintain all services necessary to host the SaaS Platform and the licensed software from the Hosting Environment such that the EMS Repository shall perform as defined herein, and in accordance with the specifications, and otherwise in accordance with the Agreement ("Hosting Services").

During the Agreement term, CONTRACTOR shall provide COUNTY with the hosting services set forth in the Agreement, this Attachment J (Hosting Services Terms and Conditions), and Exhibit A (Statement of Work). In providing the hosting services, CONTRACTOR shall achieve the service levels and performance standards set forth in Attachment B.2 (Support Services, Maintenance Services, and Service Levels), the Statements of Work, and the Agreement. The COUNTY consents to the CONTRACTOR's use of Microsoft Azure as a Subprocessor.

CONTRACTOR shall host the SaaS Platform from (i) the CONTRACTOR Primary Data Center and CONTRACTOR Secondary Data Center (as to Hosting Services not provided using a Subprocessor); (ii) all Subprocessing Availability Zones and storage, networking, and computing processing resources configured in such Subprocessing availability zones (as to Hosting Services provided using Subprocessors); and (iii) all facilities, personnel, Hosting Hardware and Hosting Software and all requirements specified in Paragraph 9.3 (Hosting Environment) ("Hosting Environment"). CONTRACTOR shall maintain a Hosting Environment to support the SaaS Platform as to the version(s) being utilized by COUNTY in accordance with Paragraph 9.3 (Hosting Environments) of this attachment.

"CONTRACTOR Primary Data Center" shall mean, as to Hosting Services not provided using a Subprocessor, the principal data center facility in which the Hosting Environment shall operate throughout the Agreement Term.

"CONTRACTOR Secondary Data Center" shall mean, as to Hosting Services not provided using a Subprocessor, a fail-over recovery data center facility, in which the Hosting Environment shall operate and provide business continuity Services throughout the Agreement Term, in the event of CONTRACTOR's inability to provide the Hosting Services from CONTRACTOR Primary Data Center.

"Subprocessing Availability Zone" shall mean a data center facility or group of data center facilities from which a Subprocessor provides storage, networking, and computing processing capability to CONTRACTOR in connection with COUNTY Confidential Information, where each Subprocessing Availability Zone is physically separated from all other Subprocessing Availability Zones, such that the services provided by the Subprocessor can be failed over from one Subprocessing Availability Zone to another Subprocessing Availability Zone in the event of a failure or issue at the first Subprocessing Availability Zone.

B. Use of Cookies on the Service

CONTRACTOR shall not use "cookies" or any other online tracking technology for purposes of discovering the identity of any users (unless CONTRACTOR is specifically authorized hereunder to obtain such information) or tracking the activities of a user after they leave the hosting services. Information collected from cookies shall constitute COUNTY Confidential Information and shall be subject to the protections provided in the Agreement. In no event shall such information be sold or otherwise made available to any third-party. CONTRACTOR shall use cookies in connection with the services provided hereunder solely for purposes of fulfilling its obligations hereunder. CONTRACTOR shall not use cookies from any third-party in delivering the services provided hereunder. A user's refusal to accept a cookie shall not preclude that user from fully utilizing the functionality of the hosting services. For purposes of the Agreement, a "cookie" shall mean any data that a server on the world wide web stores on a client system. When a user returns to the same web site, the browser sends a copy of the cookie back to the server for administrative purposes. For the avoidance of doubt, this provision shall not be applicable to CONTRACTOR's marketing-oriented commercial websites (such as www.eso.com).

9.2 OPERATIONS AND HOSTING SERVICES

A. Hosting Hardware Maintenance

CONTRACTOR shall schedule and perform maintenance (as to Hosting Services not provided using Subprocessors) and shall ensure that appropriate maintenance is performed (as to Hosting Services provided using Subprocessors), including preventive maintenance of hardware and equipment of any nature (e.g., servers, networking equipment, switches, routers, power infrastructure), utilized in the Hosting Environment to provide the Hosting Services ("Hosting Hardware"), including, but not be limited to, the repair or replacement of all (i) non-functioning or under-performing Hosting Hardware or (ii) Hosting Hardware no longer supported by its manufacturer and used by CONTRACTOR for hosting the SaaS Platform, in order to maintain the Service Levels and compatibility with the SaaS Platform, and any revisions to the SaaS Platform, and/or Interfaces.

Based on Hosting Hardware platforms (as to Hosting Services not provided using Subprocessors) and logical environment configurations (as to Hosting Services provided using Subprocessors) recommended by CONTRACTOR, CONTRACTOR shall maintain compatibility of the Hosting Services and SaaS Platform with new Hosting Hardware, all software of any nature (e.g. operating systems, presentation layer software, database software, applications, utilities, tools, firmware and security) utilized in the Hosting Environment to provide the Hosting Services ("Hosting Software"), third party products, and configurations.

B. Preventative Maintenance

CONTRACTOR shall create a schedule of required preventative maintenance tasks for the Hosting Environment (as to Hosting Services not provided using Subprocessors), and shall otherwise be responsible for the performance of preventative maintenance tasks for the Hosting Environment, to ensure that the Hosting Environment and all components thereof are functioning in accordance with the Agreement. Such preventative maintenance tasks include, but are not limited to, the following:

1. Revisions for Licensed Software, Interfaces, and Hosting Revisions for Hosting Software; and

2. Review of Error and other logs to ensure any maintenance required to correct any Errors and restore the Hosting Environment to normal operations is detected and performed in a timely manner and that such information is used to anticipate Errors and make proactive Hosting Error Corrections.

9.3 HOSTING ENVIRONMENT

A. COUNTY acknowledges that Hosting Services shall include the provision of a Hosting Environment to perform in accordance with the standard terms and service levels for Azure.

1. Hosting Environment for Hosting Services provided using Subprocessors

As to Hosting Services provided using Subprocessors, CONTRACTOR will provide the Hosting Services from Subprocessing Availability Zones as described in this Sub-paragraph 9.3.B.3 (Hosting Environment for Hosting Services provided using Subprocessors).

The Hosting Services are provided using Azure Commercial to support physical redundancy of infrastructure. The Hosting Environment:

B. Physical Security Environment

As to Hosting Services not provided using Subprocessors, CONTRACTOR shall implement the following security controls for the CONTRACTOR Primary Data Center and CONTRACTOR Secondary Data Center:

1. CONTRACTOR shall maintain COUNTY's Hosting Environment in Statement on Standards for Attestation Engagements ("SSAE") 18 certified facilities, or facilities of successor certification, with, as to each Data Center:

   a. Access controlled through documented procedures;

   b. 24x7x365 security and technical engineering staff;

   c. Physical access which requires government-issued picture identifications for access validation and multi-factor authentication for floor access;

   d. Video surveillance monitoring on a 24x7x365 basis; and

   e. Access monitored through internal management and logging systems.

2. CONTRACTOR's physical environments shall be governed by strict selective restriction of access to a place or other resource ("Access Control") for physical access to the environments. All data and storage cabinets will be contained within CONTRACTOR data centers with access only granted to those with a related job responsibility. Both CONTRACTOR data centers and the facilities in which they are housed are secured with locks that require proximity cards for physical access.

3. CONTRACTOR shall maintain comprehensive security policies, procedures, and controls to govern, support, and secure the Hosting Environment. Security policies and procedures shall be reviewed and updated on a regular basis. CONTRACTOR's security management controls shall be reviewed by an independent third- party firm, on an annual basis, following SSAE 18 or successor certification, guidelines, and format.

C. Hosting Environment Security and WAN Connectivity

CONTRACTOR shall use appropriate technology to protect COUNTY Confidential Information, COUNTY Data and Personal Data and the users of the Hosting Services in its storage and transmission between the user and the Hosting Environment, which shall include the following:

1. WAN Connectivity including (i) as to Hosting Services not provided using Subprocessors, primary and secondary communications

circuits between the CONTRACTOR Primary Data Center and CONTRACTOR Secondary Data Center and dual points of demarcation at COUNTY; and (ii) as to Hosting Services provided using Subprocessors, the Hosting Services environment will reside in Azure. CONTRACTOR will access the environment utilizing a secure VPN with a minimum of AES 128 bit encryption.

2. A network structure protected by redundant clustered firewalls and monitored with intrusion prevention systems. The firewall logs shall be reviewed weekly by enterprise security management systems to identify security threats. The Hosting Environment shall be safeguarded using Network Address Translation ("NAT"), Internet Protocol (IP) masquerading, port redirection, non-routable IP addressing and Access Control lists, multi-factor authentication, and management network segregation.

3. Background investigations will be performed in accordance with CONTRACTOR's policies and procedures for all CONTRACTOR personnel performing work at CONTRACTOR's sites under the Agreement. All CONTRACTOR's hosting and support staff shall go through CONTRACTOR's security and privacy training prior to being provided (i) physical access to the CONTRACTOR Primary Data Center or CONTRACTOR Secondary Data Center (as to Hosting Services not provided using Subprocessors), or (ii) administrator access to cloud infrastructure resources (as to Hosting Services provided using Subprocessors).

4. Multi-factor authentication to access managerial functionality within the environment for administrative access. All user access shall be monitored and managed by the CONTRACTOR's security/compliance department. All (i) servers and Hosting Hardware devices (as to Hosting Services not provided using Subprocessors); (ii) logical cloud resources (as to Hosting Services provided using Subprocessors); and (iii) software applications, user accounts, security devices, and technical services shall be fully audited and managed by enterprise management and notification systems. Any account, physical, environmental, or security change shall be identified and trigger a notification to all CONTRACTOR hosting and security staff.

5. The maintenance of security by restricting access points to all production environments. Strong password rules shall be enforced, and the Hosting Environment shall be programmatically updated to the vendor-recommended patch levels for security. The Hosting Environment shall be hardened by disabling any non-critical ports, users, protocols, and processes, following industry standards for security.

6. Operations to identify and manage risks and vulnerabilities that could affect the CONTRACTOR's ability to provide reliable Hosting

Services to COUNTY. These processes shall require CONTRACTOR management to assign a risk profile to all assets within the Hosting Environment, including Hosting Hardware, software, services, staff, and client data. Each asset and its applicable risk and vulnerabilities shall be tracked, monitored, and reviewed on a regular basis. Any new assets shall be evaluated based upon a risk rating formula. Appropriate members of CONTRACTOR's staff shall meet periodically to discuss the risks CONTRACTOR is facing. These shall include various aspects of financial and technological risks, including risks introduced by changes in the nature of services provided and processing when applicable.

7. Extensive change management policies, procedures, and controls. All non-routine environment changes shall require approvals, appropriate testing, backout plans, and sufficient documentation prior to being implemented within the hosting environment.

8. Extensive incident management and monitoring procedures for the hosting environment. CONTRACTOR shall notify COUNTY of any material attacks or service interruption impacting the servers (as to Hosting Services not provided using Subprocessors), logical cloud resources (as to Hosting Services provided using Subprocessors), or other elements of the Hosting Services in accordance with the requirements of the Agreement, including Attachment B.2 (Support Services, Maintenance Services, and Service Levels), Exhibit M of the Agreement (Information Security Requirements), Attachment I (BC/DR Requirements), and Exhibit L of the Agreement (Business Associate Agreement under the Health Insurance Portability and Accountability act of 1996).

D. Hosting Revisions

1. Other than the SaaS Platform fees, there shall be no other change or cost to COUNTY associated with hosting revisions.

2. Any hosting revisions are expected to comply with federal and state laws and regulations at no additional cost over the monthly SaaS Platform fees under the Agreement.

3. CONTRACTOR shall provide COUNTY with hosting revisions, revised related Documentation, and, if necessary, modified procedures, to correct any failure of the Hosting Environment to operate in accordance with the Specifications.

10 ATTACHMENT K - EMS REPOSITORY FUNCTIONAL REQUIREMENTS

10.1. ACCESS

a. The system shall be accessed via the internet through a web browser.

b. Users shall be able to view data on a read-only screen.
c. The system will allow the user to search patient records without closing the current record. The open records must be available in multiple screens.
d. The system will have the capability to search and browse existing patient records using user defined criteria.
e. The system must have the capability to allow users to search contents of patient records.

10.2. DATA IMPORT – THE EMS REPOSITORY SHALL HAVE THE CAPABILITY TO:

a. Import all data element/variables listed in the LA EMS Data Dictionary.
b. Import at least 800,000 records annually.
c. Provide an import log that shows how many accounts were successfully imported each time an import is conducted.
d. Provide an import log that shows how many accounts were rejected or failed.
e. Provide an import log that shows how many accounts received "warning" alert.

10.3 DATA EXPORT

a. The system must be able to submit data to the CEMSIS in the latest NEMSIS Standard.
b. The system must be able to provide an export log that shows how many records were exported.

10.4 REPORTING

a. Reports must be viewable on screen, printed and saved as files in several different formats (including Microsoft Excel).
b. The EMS Repository and Insights Reporting Platform shall have the capability to:
    1. Generate reports on the total patient population and on all data variables/elements captured for each patient.
    2. Query within a specified date range.
    3. Query subsets of patient records from the system using filters that are attached to the report.
    4. Provide online reporting capability to authorized County system managers for necessary review and accountability.
    5. Provide data submission error and exception reports.
    6. Provide ad hoc and standard query capabilities.
    7. Provide the ability to view previously generated reports by all users or by specific users.
    8. Provide capability to schedule reports to run automatically.
    9. Generate schematron failure exception reports that identify records meeting user defined exception rules.
    10. Allow print preview of all reports before printing and have print screen and selective page(s) print functionally.

11. Have a printer setting dialogue box that provides the user control over several aspects of the report's appearance.
12. Allow for user-friendly end-use report creation without requiring technical staff or expertise to create and publish reports within the modules.
13. Break down a large report into a series of related sub-reports to allow the user to run separate reports for a changing variable, such as hospital or EMS Provider. For example, the EMS Agency is running a final hospital destination by patient type (Advanced Life Support vs Basic Life Support), this typically will generate a single report of the entire database. By creating an EMS Provider sub-report, the EMS Agency can easily generate separate individual reports by EMS Provider. On Excel export, this can be displayed as different worksheet tabs in an Excel file.
14. Yield summary reports, which are statistical summaries of the database.
15. Yield listing reports, which produce a list of raw data for the patient, a group of patients or the entire database.
16. Display reports as a table (cross tabulation), chart or graph.
17. Display raw numbers and percentages on a cross tabulation table. It must be able to display a cell's percentage of patients from its row, percentage of patient from its column, or percentage of the entire report's grand total. It must also display a row and column's percentage of the report's grand total.
18. List patients and variables that fail to meet data collection requirements (i.e., blanks, not documented).
19. Customize user reports and users control the position of the report's variable on a printed page.
20. Save reports that are created and opened at any time for viewing, running and modification.
21. Generate predefined reports.
22. Provide search function to locate previously saved and stored created reports as well as the report output (tables, charts and graphs).
23. Group reports by report type.
24. Calculate differences between like variables (e.g., calculate time duration between different time fields).
25. Exclude and include variable with Blank, Not Documented and Not Applicable entries.
26. Display abbreviated and full text names of each variable that exist in the database.
27. Report on numeric variables. The user must be able to group numeric variables into ranges (i.e., a report utilizing age would typically provide a report listing all individual ages (0 years through 120 years), the system must have the capability to group ages such that the report can be customized to report on age 0-10 years, 11-20 years, etc.).
28. Sort variables in ascending or descending order.

29. Generate reports containing two variables in a cross-tabulation format such that both raw numbers and percentages are displayed. The system must be able to display a cell's percentage of patients from its row, percentage of patient from its column, or percentage of the entire report's grand total. It can also display a row or a column's percentage of the report's grand total.
30. Generate reports containing multiple variables and the capability to sort by variable.
31. Link variables associated with other variables. For example, to run a report on response time, a user might create a report table on the variable dispatch time and arrival time. Due to the variability in the number of response vehicle per incident, the user must link each arrival and dispatched time to a specific EMS response unit.
32. Subdivide reports with multiple variables using a single variable's responses and made to show counts (the number of patients that match a given response) and totals (the sum of numeric variables in records matching a given response) for each individual response. For example, if a user creates a report that show the Insurance Company and the Total Charges for each patient, the system must be able to show the number of patients having each type of insurance as well as the total amount owed to the provider by each insurer.
33. Collect, query and report on user specified patient care issues and quality improvement filters.
34. Have a printer setting dialogue box that provides the user control over several aspects of a report's appearance, such as whether or not a cover page is included, and what information is printed on the pages of the report itself.

11 ATTACHMENT L – SUPPORT SERVICES

11.1. DEFINITIONS

Capitalized terms not defined below shall have the same meaning as in the General Terms & Conditions.

11.1.1 "Enhancement" means a modification, addition or new release of the Software that when added to the Software, materially changes its utility, efficiency, functional capability or application.

11.1.2 "E-mail Support" means ability to make requests for technical support assistance by e-mail at any time concerning the use of the then-current release of Software.

11.1.3 "Error" means an error in the Software, which significantly degrades performance of such Software as compared to CONTRACTOR's then-published Documentation.

11.1.4 "Error Correction" means the use of reasonable commercial efforts to correct Errors.

11.1.5 "Fix" means the repair or replacement of object code for the Software or Documentation to remedy an Error.

11.1.6 "Initial Response" means the first contact by a Support Representative after the incident has been logged and a ticket generated. This may include an automated email response depending on when the incident is first communicated.

11.1.7 "Management Escalation" means, if the initial Workaround or Fix does not resolve the Error, notification of management that such Error(s) have been reported and of steps being taken to correct such Error(s).

11.1.8 "Severity 1 Error" means an Error which renders the Software completely inoperative (*e.g.*, a User cannot access the Software due to unscheduled downtime or an Outage).

11.1.9 "Severity 2 Error" means an Error in which Software is still operable; however, one or more significant features or functionality are unavailable (*e.g.*, a User cannot access a core component of the Software).

11.1.10 "Severity 3 Error" means any other error that does not prevent a User from accessing a significant feature of the Software (*e.g.*, User is experiencing latency in reports).

11.1.11 "Severity 4 Error" means any error related to Documentation or a COUNTY Enhancement request.

11.1.12 "Status Update" means if the initial Workaround or Fix cannot resolve the Error, notification of the COUNTY regarding the progress of the Workaround or Fix.

11.1.13 "Online Support" means information available through CONTRACTOR's website (www.eso.com), including frequently asked questions and bug reporting via Live Chat.

11.1.14 "Support Representative" shall be CONTRACTOR employee(s) or agent(s) designated to receive Error notifications from COUNTY, which COUNTY's Administrator has been unable to resolve.

11.1.15 "Update" means an update or revision to Software, typically for Error Correction.

11.1.16 "Upgrade" means a new version or release of Software or a particular component of Software, which improves the functionality or which adds functional capabilities to the Software and is not included in an Update. Upgrades may include Enhancements.

11.1.17 "Workaround" means a change in the procedures followed or data supplied by COUNTY to avoid an Error without substantially impairing COUNTY's use of the Software.

11.2. SUPPORT SERVICES

11.2.1 COUNTY will provide at least one administrative employee (the "Administrator" or "Administrators") who will handle all requests for first-level support from COUNTY's employees with respect to the Software. Such support is intended to be the "front line" for support and information about the Software to COUNTY's Users. CONTRACTOR will provide training, documentation, and materials to the Administrator to enable the Administrator to provide technical support to COUNTY's Users. The Administrator will notify a Support Representative of any Errors that the Administrator cannot resolve and assist CONTRACTOR in information gathering.

11.2.2 CONTRACTOR will provide Support Services consisting of (a) Error Correction(s); Enhancements, Updates and Upgrades that CONTRACTOR, in its discretion, makes generally available to its customers without additional charge; and (c) E-mail Support, telephone support, and Online Support. CONTRACTOR may use multiple forms of communication for purposes of submitting periodic status reports to COUNTY, including but not limited to, messages in the Software, messages appearing upon login to the Software or other means of broadcasting Status Update(s) to multiple customers affected by the same Error, such as a customer portal.

11.2.3 CONTRACTOR's support desk will be staffed with competent technical consultants who are trained in and thoroughly familiar with the Software and with COUNTY's applicable configuration. Telephone support and all communications will be delivered in intelligible English.

11.2.4 Normal business hours for CONTRACTOR's support desk are Monday through Friday 6:00 am to 6:00 pm Pacific Time. COUNTY will receive a call back from a Support Representative after-hours for a Severity 1 Error.

11.3. ERROR PRIORITY LEVELS. COUNTY will report all Errors to CONTRACTOR via e-mail (support@eso.com) or by telephone (866-766-9471, option #3). CONTRACTOR shall exercise commercially reasonable efforts to correct any Error reported by COUNTY in accordance with the priority level reasonably assigned to such Error by CONTRACTOR. Should CONTRACTOR discover the Error, it will notify COUNTY through its regular processes. If COUNTY determines, in its reasonable assessment of the Error, that the Severity Level needs to be escalated to a higher level, COUNTY will meet with CONTRACTOR to discuss the escalation need, and CONTRACTOR shall be required to reasonably escalate.

11.3.1 Severity 1 Error. CONTRACTOR shall (i) commence Error Correction promptly; (ii) provide an Initial Response within four hours; (iii) initiate Management Escalation promptly; and (iv) provide COUNTY with a Status Update within four hours if CONTRACTOR cannot resolve the Error within four hours.

11.3.2 Severity 2 Error. CONTRACTOR shall (i) commence Error Correction promptly; (ii) provide an Initial Response within eight hours; (iii) initiate Management Escalation within 48 hours if unresolved; and (iv) provide COUNTY with a Status Update within forty-eight hours if CONTRACTOR cannot resolve the Error within forty-eight hours.

11.3.3 Severity 3 Error. CONTRACTOR shall (i) commence Error Correction promptly; (ii) provide an Initial Response within three business days; and (iii) provide COUNTY with a Status Update within seven calendar days if CONTRACTOR cannot resolve the Error within seven calendar days.

11.3.4 Severity 4 Error. CONTRACTOR shall (i) provide an Initial Response within seven calendar days.

11.4. EXCLUSIONS

11.4.1 CONTRACTOR shall have no obligation to perform Error Corrections or otherwise provide support for: (i) COUNTY's repairs, maintenance or modifications to the Software (if permitted); (ii) COUNTY's misapplication or unauthorized use of the Software; (iii) altered or damaged Software not caused by CONTRACTOR; (iv) any third-party software; (v) hardware issues; (vi) COUNTY's breach of the Agreement; and (vii) any other causes beyond the CONTRACTOR's reasonable control.

11.4.2 CONTRACTOR shall have no liability for any changes in COUNTY's hardware or software systems that may be necessary to use the Software due to a Workaround or Fix.

11.4.3 CONTRACTOR is not required to perform any Error Correction unless CONTRACTOR can replicate such Error on its own software and hardware or through remote access to COUNTY's software and hardware.

11.4.4 COUNTY is solely responsible for its selection of hardware, and CONTRACTOR shall not be responsible for the performance of such hardware even if CONTRACTOR makes recommendations regarding the same. However, CONTRACTOR can only make recommendations that are compatible for use with the System.

* * * * *

EXHIBIT B

SCHEDULE OF PAYMENTS
(ADDED UNDER AMENDMENT NUMBER TWELVE)

SEPTEMBER 2023

I. CONTRACT YEAR ONE (2001 – 2002):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$257,500.00
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$28,176.67	$338,120.04
SUBTOTAL		**$595,620.04**

II. CONTRACT YEAR TWO (2002 – 2003):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$265,225.00
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$29,021.97	$348,263.64
SUBTOTAL		**$613,488.64**

III. CONTRACT YEAR THREE (2003 – 2004):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$273,181.75
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$29,892.63	$358,711.56
SUBTOTAL		**$631,893.31**

IV. CONTRACT YEAR FOUR (2004 – 2005):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$281,377.20
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$30,789.40	$369,472.80
SUBTOTAL		**$650,850.00**

V. CONTRACT YEAR FIVE (2005 – 2006):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$289,818.52
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$31,713.09	$380,557.08
SUBTOTAL		**$670,375.60**

VI. CONTRACT YEAR SIX (2006 – 2007):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$298,513.07
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$32,664.48	$391,973.76
SUBTOTAL		**$690,486.83**

VII. CONTRACT YEAR SEVEN (2007 – 2008):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$307,468.47

B. TEMIS Application Software Support Services: Fixed Monthly Fee	$33,644.41	$403,732.92
SUBTOTAL		**$711,201.39**

VIII. CONTRACT YEAR EIGHT (2008 – 2009):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$316,692.52
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$34,653.75	$415,845.00
SUBTOTAL		**$732,537.52**

IX. CONTRACT YEAR NINE (2009 – 2010):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$326,193.30
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$35,693.36	$428,320.32
SUBTOTAL		**$754,513.62**

X. CONTRACT YEAR TEN (2010 – 2011):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$335,979.09
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$36,764.16	$441,169.92
C. Upgraded TEMIS Application Software		Up to $293,250.00
1. TEMIS Database Consolidation [(1)]		One Time Fee up to $120,000.00
2. TEMIS FTP Solution [(2)]		One Time Fee up to $50,000.00
a. FTP Set-up at Central Site to Receive Data		$4,000.00
b. FTP Set-up at Field Sites (46 sites at $1,000.00 each)		$46,000.00
3. TEMIS ePCR Pilot [(3)]		One Time Fee (Optional) up to $28,000.00
a. Per installation to a maximum of 5 stations (one installation)		$25,000.00
b. Each additional station (2 stations at $1,500.00 each)		$3,000.00
4. TEMIS Scanning Solution [(4)]		One Time Fee (Optional) up to $95,250.00
a. Per installation to a maximum of 5 stations (two installations)		$50,000.00
b. Each additional station (24 stations at $1,500.00 each)		$36,500.00
c. Scanning Engine		$4,500.00
d. Scannable Form Development		$4,250.00
SUBTOTAL (up to)		**$1,070,399.01**

GRAND TOTAL FOR TEN YEARS:

A. TEMIS Application Software License Fee	$2,951,948.92
B. TEMIS Application Software Support Services Fee	$3,876,167.04
C. Upgraded TEMIS Application Software	Up to $293,250.00
GRAND TOTAL FOR YEARS ONE THROUGH TEN (Contract Sum up to)	**$7,121,365.96**

XI. CONTRACT YEAR ELEVEN (2011 – 2012):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$346,058.46
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$37,867.08	$454,404.96
SUBTOTAL FOR YEAR ELEVEN		**$800,463.42**
GRAND TOTAL FOR YEARS ONE THROUGH ELEVEN (Contract Sum up to)		**$7,921,829.38**

XII. CONTRACT YEAR TWELVE (2012 – 2013):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$356,440.21
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$39,003.09	$468,037.08
SUBTOTAL FOR YEAR TWELVE (up to)		**$824,477.29**
GRAND TOTAL FOR YEARS ONE THROUGH TWELVE (Contract Sum up to)		**$8,746,306.67**

XIII CONTRACT YEAR THIRTEEN (2013 – 2014):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$367,133.41
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$40,173.18	$482,078.16
SUBTOTAL FOR YEAR THIRTEEN (up to)		**$849,211.57**
GRAND TOTAL FOR YEARS ONE THROUGH THIRTEEN (Contract Sum up to)		**$9,595,518.24**

XIV. CONTRACT YEAR FOURTEEN (2014 – 2015):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$378,148.02
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$41,378.37	$496,540.44
SUBTOTAL FOR YEAR FOURTEEN (up to)		**$874,688.46**
GRAND TOTAL FOR YEARS ONE THROUGH FOURTEEN (Contract Sum up to)		**$10,470,206.70**

XV. CONTRACT YEAR FIFTEEN (2015 – 2016):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$389,492.46
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$42,619.72	$511,436.65
SUBTOTAL FOR YEAR FIFTEEN (up to)		**$900,929.11**
GRAND TOTAL FOR YEARS ONE THROUGH FIFTEEN (Contract Sum up to)		**$11,371,135.81**

XVI. CONTRACT YEAR SIXTEEN (2016 – 2017):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$401,177.23
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$43,898.31	$526,779.72
SUBTOTAL FOR YEAR SIXTEEN (up to)		**$927,956.95**

GRAND TOTAL FOR YEARS ONE THROUGH SIXTEEN (Contract Sum up to) $12,299,092.76

XVII. CONTRACT YEAR SEVENTEEN (2017 – 2018):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$413,212.55
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$45,215.26	$542,583.12
SUBTOTAL FOR YEAR SEVENTEEN (up to)		**$955,795.67**

GRAND TOTAL FOR YEARS ONE THROUGH SEVENTEEN (Contract Sum up to) $13,254,888.43

XVIII. CONTRACT YEAR EIGHTEEN (2018 – 2019):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$425,608.93
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$46,571.72	$588,860.64
SUBTOTAL FOR YEAR EIGHTEEN (up to)		**$984,469.57**

GRAND TOTAL FOR YEARS ONE THROUGH EIGHTEEN (Contract Sum up to) $14,239,358

XIX. CONTRACT YEAR NINETEEN (2019 – 2020):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$438,377.19
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$47,968.87	$575,626.44
SUBTOTAL FOR YEAR NINETEEN (up to)		**$1,014,003.63**

GRAND TOTAL FOR YEARS ONE THROUGH NINETEEN (Contract Sum up to) $15,253,361

XX. CONTRACT YEAR TWENTY (2020 – 2021):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$451,528.50
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$49,407.93	$592,895.16
SUBTOTAL FOR YEAR TWENTY (up to)		**$1,044,423.66**

GRAND TOTAL FOR YEARS ONE THROUGH TWENTY (Contract Sum up to) $16,297,785

XXI. CONTRACT YEAR TWENTY-ONE (2021 – 2022):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee	NA	$465,074.35
B. TEMIS Application Software Support Services: Fixed Monthly Fee	$50,890.16	$610,682.92
SUBTOTAL FOR YEAR TWENTY-ONE (up to)		**$1,075,756.20**

GRAND TOTAL FOR YEARS ONE THROUGH TWENTY-ONE (Contract Sum up to) $17,373,542

XXII. CONTRACT YEAR TWENTY-TWO (A) (6-Month Period of 7/1/2022 through 12/31/2022):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee [5]	NA	$239,513.29
B. TEMIS Application Software Support Services: Fixed Monthly Fee [6]	$52,416.86	$314,501.16
SUBTOTAL FOR YEAR TWENTY-TWO (A) (up to)		**$554,014.45**

GRAND TOTAL FOR YEARS ONE THROUGH TWENTY-TWO (A) (Contract Sum up to) $17,927,556.45

XXIII. CONTRACT YEAR TWENTY-TWO (B) (6-Month Period of 1/1/2023 through 6/30/2023)

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee [7]	NA	$239,513.29
B. TEMIS Application Software Support Services: Fixed Monthly Fee [8]	$52,416.86	$314,501.16
SUBTOTAL FOR YEAR TWENTY-TWO (B) (up to)		**$554,014.45**

GRAND TOTAL FOR YEARS ONE THROUGH TWENTY-TWO (Contract Sum up to) $18,481,570.90

XXIV. CONTRACT YEAR TWENTY-THREE (3-Month Period of 7/1/2023 through 9/30/2023):

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee [9]	NA	$123,349.35
B. TEMIS Application Software Support Services: Fixed Monthly Fee [10]	$53,989.39	$161,968.17
SUBTOTAL FOR YEAR TWENTY-THREE (Contract Sum up to)		**$285,317.52**

GRAND TOTAL FOR YEARS ONE THROUGH TWENTY-THREE (Contract Sum up to) $18,766,888.42

THREE-YEAR EXTENSION

XXIV. CONTRACT YEAR TWENTY-THREE/TWENTY-FOUR (10/1/2023 through 9/30/2024)

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee Legacy Product (Fire Rescue, LA Base, LA Trauma)		$558,088.00
B. TEMIS Application Software Support Services: Monthly Fee Legacy Product (Fire Rescue, LA Base, LA Trauma)	$61,068.00	$732,816.00
C. EMS Repository NEMSIS Standard: One-Time Fee[11]		$140,000.00
D. EMS Repository NEMSIS Standard: Recurring Fee[11]		$300,000.00
E. Insights Reporting Platform[11]		$75,000.00
F. Pool Dollars for Additional Work[12]		$787,501.00
SUBTOTAL FOR YEAR TWENTY-THREE/TWENTY-FOUR (up to)		**$2,593,404.90**

GRAND TOTAL FOR YEARS ONE THROUGH TWENTY-THREE/TWENTY-FOUR (Contract Sum up to) $21,360,293.32

XXV. CONTRACT YEAR TWENTY-FOUR/TWENTY-FIVE (10/1/2024 through 9/30/2025)

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee Legacy Product (LA Base, LA Trauma)		$561,576.00
B. TEMIS Application Software Support Services: Monthly Fee	$61,450.00	$737,400.00
C. Legacy Product (LA Base, LA Trauma)		
D. EMS Repository NEMSIS 3.5 Standard: Recurring Fee[11]		$315,000.00
E. Insights Reporting Platform[11]		$78,750.00
F. Pool Dollars for Additional Work[12]		**(see Footnote 12)**
SUBTOTAL FOR YEAR TWENTY-FOUR/TWENTY-FIVE (up to)		**$1,692,726.00**

GRAND TOTAL FOR YEARS ONE THROUGH TWENTY-FOUR/TWENTY-FIVE (Contract Sum up to) $23,053,019.32

XXVI. CONTRACT YEAR TWENTY-FIVE/TWENTY-SIX (10/1/2025 through 9/30/2026)

	MONTHLY FEE	TOTAL ANNUAL FEE
A. TEMIS Application Software: Fixed Annual License Fee Legacy Product (LA Base, LA Trauma)		$578,423.00
B. TEMIS Application Software Support Services: Monthly Fee	$63,293.00	$759,516.00
C. Legacy Product (LA Base, LA Trauma)		
D. EMS Repository NEMSIS 3.5 Standard: Recurring Fee[11]		$330,750.00
E. Insights Reporting Platform[11]		$82,687.00
F. Pool Dollars for Additional Work[12]		**(see Footnote 12)**
SUBTOTAL FOR YEAR TWENTY-FIVE/TWENTY-SIX (up to)		**$1,751,376.00**

GRAND TOTAL FOR YEARS ONE THROUGH TWENTY-FIVE/TWENTY-SIX (Contract Sum up to) $24,804,395.00

(1) Consist of software development to combine the current three TEMIS databases (LA Fire-Rescue, LA Base and LA Trauma) into one central database.

(2) Develop and install a File Transfer Protocol (FTP) site for transfer of confidential patient care records which consist of two phases; installation and set-up at the TEMIS Central Site and 46 TEMIS Field Sites.

(3) Optional Project: Develop and implement a pilot project with one EMS Provider Agency consisting of electronic data capture utilizing an electronic patient care record (ePCR).

(4) Optional Project: Develop and implement a pilot project with one EMS Provider Agency and the TEMIS Central Site consisting of electronic data capture utilizing a scanning solution to convert the paper patient care record into electronic data.

(5) The "Total Annual Fee" for Contract Year Twenty-Two (A) that is reflected in "TEMIS Application Software: Fixed Annual License Fee" is based on the 6-month period of 7/1/2022 through 12/31/2022.

(6) The "Monthly Fee" and "Total Annual Fee" for Contract Year Twenty-Two (A) that are reflected in "TEMIS Application Software Support Services: Fixed Monthly Fee" are based on the 6-month period of 7/1/2022 through 12/31/2022.

(7) The "Total Annual Fee" for Contract Year Twenty-Two (B) that is reflected in "TEMIS Application Software: Fixed Annual License Fee" is based on the 6-month period of 1/1/23 through 6/30/23.

(8) The "Monthly Fee" and "Total Annual Fee" for Contract Year Twenty-Two (B) that are reflected in "TEMIS Application Software Support Services: Fixed Monthly Fee" are based on the 6-month period of 1/1/23 through 6/30/23.

(9) The "Total Annual Fee" for Contract Year Twenty-Three that is reflected in "TEMIS Application Software: Fixed Annual License Fee" are based on the 3-month period of 7/1/23 through 09/30/23.

(10) The "Monthly Fee" and "Total Annual Fee" for Contract Year Twenty-Three that are reflected in "TEMIS Application Software Support Services: Fixed Monthly Fee" are based on the 3-month period of 7/1/23 through 9/30/23.

(11) Fees for these items to be paid annually in advance, with the invoice due October 15 of the applicable Contract Year.

(12) Pool Dollars in the amount of $787,501 for Additional Work shall be available for use during Contract Year Twenty-Three/Twenty-Four through Contract Year Twenty-Five/Twenty-Six (10/1/2023 – 9/30/2026).

CONTRACTOR EMPLOYEE ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

x

(Note: This certification is to be executed and returned to County with Contractor's executed Contract. Work cannot begin on the Agreement until County receives this executed document.)

Contractor Name _____ Agreement No._____
Employee Name _____

GENERAL INFORMATION:

Your employer referenced above has entered into an Agreement with the County of Los Angeles to provide certain services to the County. The County requires your signature on this Contractor Employee Acknowledgement and Confidentiality Agreement.

EMPLOYEE ACKNOWLEDGEMENT:

I understand and agree that the Contractor referenced above is my sole employer for purposes of the above-referenced contract. I understand and agree that I must rely exclusively upon my employer for payment of salary and any and all other benefits payable to me or on my behalf by virtue of my performance of work under the above-referenced contract.

I understand and agree that I am not an employee of the County of Los Angeles for any purpose whatsoever and that I do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced contract. I understand and agree that I do not have and will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

I understand and agree that I may be required to undergo a background and security investigation(s). I understand and agree that my continued performance of work under the above-referenced Agreement is contingent upon my passing, to the satisfaction of the County, any and all such investigations. I understand and agree that my failure to pass, to the satisfaction of the County, any such investigation shall result in my immediate release from performance under this and/or any future contract.

CONFIDENTIALITY AGREEMENT:

I may be involved with work pertaining to services provided by the County of Los Angeles and, if so, I may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, I may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. I understand that if I am involved in County work, the County must ensure that I, too, will protect the confidentiality of such data and information. Consequently, I understand that I must sign this agreement as a condition of my work to be provided by my employer for the County. I have read this agreement and have taken due time to consider it prior to signing.

I hereby agree that I will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced Agreement between my employer and the County of Los Angeles. I agree to forward all requests for the release of any data or information received by me to my immediate supervisor.

CONTRACTOR EMPLOYEE ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

I agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information and all other original materials produced, created, or provided to or by me under the above-referenced contract. I agree to protect these confidential materials against disclosure to other than my employer or County employees who have a need to know the information. I agree that if proprietary information supplied by other County vendors is provided to me during this employment, I shall keep such information confidential.

I agree to report to my immediate supervisor any and all violations of this agreement by myself and/or by any other person of whom I become aware. I agree to return all confidential materials to my immediate supervisor upon completion of this Agreement or termination of my employment with my employer, whichever occurs first.

I acknowledge that violation of this agreement may subject me to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

SIGNATURE: _____ DATE: ____/____/____

PRINTED NAME: _____

POSITION: _____

CONTRACTOR NON-EMPLOYEE ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

(Note: This certification is to be executed and returned to County with Contractor's executed Contract. Work cannot begin on the Agreement until County receives this executed document.)

Contractor Name _____ Agreement No._____

Non-Employee Name _____

GENERAL INFORMATION:

The Contractor referenced above has entered into an Agreement with the County of Los Angeles to provide certain services to the County. The County requires your signature on this Contractor Non-Employee Acknowledgement and Confidentiality Agreement.

NON-EMPLOYEE ACKNOWLEDGEMENT:

I understand and agree that the Contractor referenced above has exclusive control for purposes of the above-referenced contract. I understand and agree that I must rely exclusively upon the Contractor referenced above for payment of salary and any and all other benefits payable to me or on my behalf by virtue of my performance of work under the above-referenced contract.

I understand and agree that I am not an employee of the County of Los Angeles for any purpose whatsoever and that I do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced contract. I understand and agree that I do not have and will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

I understand and agree that I may be required to undergo a background and security investigation(s). I understand and agree that my continued performance of work under the above-referenced Agreement is contingent upon my passing, to the satisfaction of the County, any and all such investigations. I understand and agree that my failure to pass, to the satisfaction of the County, any such investigation shall result in my immediate release from performance under this and/or any future contract.

CONFIDENTIALITY AGREEMENT:

I may be involved with work pertaining to services provided by the County of Los Angeles and, if so, I may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, I may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. I understand that if I am involved in County work, the County must ensure that I, too, will protect the confidentiality of such data and information. Consequently, I understand that I must sign this agreement as a condition of my work to be provided by the above-referenced Contractor for the County. I have read this agreement and have taken due time to consider it prior to signing.

CONTRACTOR NON-EMPLOYEE ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

I hereby agree that I will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced Agreement between the above-referenced Contractor and the County of Los Angeles. I agree to forward all requests for the release of any data or information received by me to the above-referenced Contractor.

I agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information, and all other original materials produced, created, or provided to or by me under the above-referenced contract. I agree to protect these confidential materials against disclosure to other than the above-referenced Contractor or County employees who have a need to know the information. I agree that if proprietary information supplied by other County vendors is provided to me, I shall keep such information confidential.

I agree to report to the above-referenced Contractor any and all violations of this agreement by myself and/or by any other person of whom I become aware. I agree to return all confidential materials to the above-referenced Contractor upon completion of this Agreement or termination of my services hereunder, whichever occurs first.

I acknowledge that violation of this agreement may subject me to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

SIGNATURE: _____ DATE: ____/____/____

PRINTED NAME: _____

POSITION: _____

BUSINESS ASSOCIATE AGREEMENT UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("HIPAA")

County is a Covered Entity as defined by, and subject to the requirements and prohibitions of, the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), and regulations promulgated thereunder, including the Privacy, Security, Breach Notification, and Enforcement Rules at 45 Code of Federal Regulations (C.F.R.) Parts 160 and 164 (collectively, the "HIPAA Rules").

Contractor performs or provides functions, activities or services to County that require Contractor in order to provide such functions, activities or services to create, access, receive, maintain, and/or transmit information that includes or that may include Protected Health Information, as defined by the HIPAA Rules. As such, Contractor is a Business Associate, as defined by the HIPAA Rules, and is therefore subject to those provisions of the HIPAA Rules that are applicable to Business Associates.

The HIPAA Rules require a written agreement ("Business Associate Agreement") between County and Contractor in order to mandate certain protections for the privacy and security of Protected Health Information, and these HIPAA Rules prohibit the disclosure to or use of Protected Health Information by Contractor if such an agreement is not in place.

This Business Associate Agreement and its provisions are intended to protect the privacy and provide for the security of Protected Health Information disclosed to or used by Contractor in compliance with the HIPAA Rules.

Therefore, the parties agree as follows:

1. DEFINITIONS

1.1 "Breach" has the same meaning as the term "breach" at 45 C.F.R. § 164.402.

1.2 "Business Associate" has the same meaning as the term "business associate" at 45 C.F.R. § 160.103. For the convenience of the parties, a "business associate" is a person or entity, other than a member of the workforce of covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to Protected Health Information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of another business associate. And in reference to the party to this Business Associate Agreement "Business Associate" shall mean Contractor.

1.3 "Covered Entity" has the same meaning as the term "covered entity" at 45 C.F.R. § 160.103, and in reference to the party to this Business Associate Agreement, "Covered Entity" shall mean County.

1.4 "Data Aggregation" has the same meaning as the term "data aggregation" at 45 C.F.R. § 164.501.

1.5 "De-identification" refers to the de-identification standard at 45 C.F.R. § 164.514.

1.6 "Designated Record Set" has the same meaning as the term "designated record set" at 45 C.F.R. § 164.501.

1.7 "Disclose" and "Disclosure" mean, with respect to Protected Health Information, the release, transfer, provision of access to, or divulging in any other manner of Protected Health Information outside Business Associate's internal operations or to other than its workforce. (See 45 C.F.R. § 160.103.)

1.8 "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. (See 42 U.S. C. § 17921.)

1.9 "Electronic Media" has the same meaning as the term "electronic media" at 45 C.F.R. § 160.103. For the convenience of the parties, electronic media means (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

1.10 "Electronic Protected Health Information" has the same meaning as the term "electronic protected health information" at 45 C.F.R. § 160.103, limited to Protected Health Information created or received by Business Associate from or on behalf of Covered Entity. For the convenience of the parties, Electronic Protected Health Information means Protected Health

Information that is (i) transmitted by electronic media; (ii) maintained in electronic media.

1.11 "Health Care Operations" has the same meaning as the term "health care operations" at 45 C.F.R. § 164.501.

1.12 "Individual" has the same meaning as the term "individual" at 45 C.F.R. § 160.103. For the convenience of the parties, Individual means the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502 (g).

1.13 "Law Enforcement Official" has the same meaning as the term "law enforcement official" at 45 C.F.R. § 164.103.

1.14 "Minimum Necessary" refers to the minimum necessary standard at 45 C.F.R. § 164.502 (b).

1.15 "Protected Health Information" has the same meaning as the term "protected health information" at 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity. For the convenience of the parties, Protected Health Information includes information that (i) relates to the past, present or future physical or mental health or condition of an Individual; the provision of health care to an Individual, or the past, present or future payment for the provision of health care to an Individual; (ii) identifies the Individual (or for which there is a reasonable basis for believing that the information can be used to identify the Individual); and (iii) is created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity, and includes Protected Health Information that is made accessible to Business Associate by Covered Entity. "Protected Health Information" includes Electronic Protected Health Information.

1.16 "Required by Law" has the same meaning as the term "required by law" at 45 C.F.R. § 164.103.

1.17 "Secretary" has the same meaning as the term "secretary" at 45 C.F.R. § 160.103

1.18 "Security Incident" has the same meaning as the term "security incident" at 45 C.F.R. § 164.304.

1.19 "Services" means, unless otherwise specified, those functions, activities, or services in the applicable underlying Agreement, Contract, Master Agreement, Work Order, or Purchase Order or other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

1.20 "Subcontractor" has the same meaning as the term "subcontractor" at 45 C.F.R. § 160.103.

1.21 "Unsecured Protected Health Information" has the same meaning as the term "unsecured protected health information" at 45 C.F.R. § 164.402.

1.22 "Use" or "Uses" means, with respect to Protected Health Information, the sharing, employment, application, utilization, examination or analysis of such Information within Business Associate's internal operations. (See 45 C.F.R § 164.103.)

1.23 Terms used, but not otherwise defined in this Business Associate Agreement, have the same meaning as those terms in the HIPAA Rules.

2. PERMITTED AND REQUIRED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

2.1 Business Associate may only Use and/or Disclose Protected Health Information as necessary to perform Services, and/or as necessary to comply with the obligations of this Business Associate Agreement.

2.2 Business Associate may Use Protected Health Information for de-identification of the information if de-identification of the information is required to provide Services.

2.3 Business Associate may Use or Disclose Protected Health Information as Required by Law.

2.4 Business Associate shall make Uses and Disclosures and requests for Protected Health Information consistent with the Covered Entity's applicable Minimum Necessary policies and procedures.

2.5 Business Associate may Use Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities.

2.6 Business Associate may Disclose Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities, provided the Disclosure is Required by Law or Business Associate obtains reasonable assurances from the person to whom the Protected Health Information is disclosed (i.e., the recipient) that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purposes for which it was disclosed to the recipient and the recipient notifies Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached.

2.7 Business Associate may provide Data Aggregation services relating to Covered Entity's Health Care Operations if such Data Aggregation services are necessary in order to provide Services.

3. PROHIBITED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

3.1 Business Associate shall not Use or Disclose Protected Health Information other than as permitted or required by this Business Associate Agreement or as Required by Law.

3.2 Business Associate shall not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except for the specific Uses and Disclosures set forth in Sections 2.5 and 2.6.

3.3 Business Associate shall not Use or Disclose Protected Health Information for de-identification of the information except as set forth in section 2.2.

4. OBLIGATIONS TO SAFEGUARD PROTECTED HEALTH INFORMATION

4.1 Business Associate shall implement, use, and maintain appropriate safeguards to prevent the Use or Disclosure of Protected Health Information other than as provided for by this Business Associate Agreement.

4.2 Business Associate shall comply with Subpart C of 45 C.F.R Part 164 with respect to Electronic Protected Health Information, to prevent the Use or Disclosure of such information other than as provided for by this Business Associate Agreement.

5. REPORTING NON-PERMITTED USES OR DISCLOSURES, SECURITY INCIDENTS, AND BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION

5.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information not permitted by this Business Associate Agreement, any Security Incident, and/ or any Breach of Unsecured Protected Health Information as further described in Sections 5.1.1, 5.1.2, and 5.1.3.

5.1.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information by Business Associate, its employees, representatives, agents or Subcontractors not provided for by this Agreement of which Business Associate becomes aware.

5.1.2 Business Associate shall report to Covered Entity any Security Incident affecting Business Associate's systems used in the delivery of its services to Covered Entity of which Business Associate becomes aware.

5.1.3 Business Associate shall report to Covered Entity any Breach by Business Associate, its employees, representatives, agents, workforce members, or Subcontractors of Unsecured Protected Health Information that is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate, and which affects Business Associate's systems used in the delivery of its services to Covered Entity. Business Associate shall be deemed to have knowledge of a Breach of Unsecured Protected Health Information if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of Business Associate, including a Subcontractor, as determined in accordance with the federal common law of agency.

5.2 Except as provided in Section 5.3, for any reporting required by Section 5.1, Business Associate shall provide, to the extent available, all information required by, and within the times frames specified in, Sections 5.2.1 and 5.2.2.

5.2.1 Business Associate shall make a prompt telephonic report upon discovery of the non-permitted Use or Disclosure of Protected Health Information, Security Incident or Breach of Unsecured Protected Health Information to **(562) 940-3335** that minimally includes:

(a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident, or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident, or Breach, if known;
(b) The number of Individuals whose Protected Health Information is involved;
(c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident, or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);
(d) The name and contact information for a person highly knowledgeable of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident, or Breach.

5.2.2 Business Associate shall make a written report without unreasonable delay and in no event later than five (5) business days from the date of discovery by Business Associate of the non-permitted Use or Disclosure of

5.2.3 of Protected Health Information, Security Incident, or Breach of Unsecured Protected Health Information and to the **Chief HIPAA Privacy Officer at: Hall of Records, County of Los Angeles, Chief Executive Office, Risk Management Branch-Office of Privacy, 320 W. Temple Street, 7th Floor, Los Angeles, California 90012,** PRIVACY@ceo.lacounty.gov**,** that includes, to the extent possible:

(a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident, or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident, or Breach, if known;

(b) The number of Individuals whose Protected Health Information is involved;

(c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident, or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(d) The identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, Used, or Disclosed;

(e) Any other information necessary to conduct an assessment of whether notification to the Individual(s) under 45 C.F.R. § 164.404 is required;

(f) Any steps Business Associate believes that the Individual(s) could take to protect him or herself from potential harm from the non-permitted Use or Disclosure, Security Incident, or Breach;

(g) A brief description of what Business Associate is doing to investigate, to mitigate harm to the Individual(s), and to protect against any further similar occurrences; and

(h) The name and contact information for a person highly knowledgeable of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident, or Breach.

5.2.4 If Business Associate is not able to provide the information specified in Section 5.2.1 or 5.2.2 at the time of the required report, Business Associate shall provide such information promptly thereafter as such information becomes available.

5.3 Business Associate may delay the notification required by Section 5.1.3, if a law enforcement official states to Business Associate that notification would impede a criminal investigation or cause damage to national security.

5.3.1 If the law enforcement official's statement is in writing and specifies the time for which a delay is required, Business Associate shall delay its reporting and/or notification obligation(s) for the time period specified by the official.

5.3.2 If the statement is made orally, Business Associate shall document the statement, including the identity of the official making the statement, and delay its reporting and/or notification obligation(s) temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in Section 5.3.1 is submitted during that time.

6. WRITTEN ASSURANCES OF SUBCONTRACTORS

6.1 In accordance with 45 C.F.R. § 164.502 (e)(1)(ii) and § 164.308 (b)(2), if applicable, Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of Business Associate is made aware of its status as a Business Associate with respect to such information and that Subcontractor agrees in writing to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information.

6.2 Business Associate shall take commercially reasonable steps to cure any material breach or violation by Subcontractor of the agreement required by Section 6.1.

6.3 If the steps required by Section 6.2 do not cure the breach or end the violation, Contractor shall terminate, if feasible, any arrangement with Subcontractor by which Subcontractor creates, receives, maintains, or transmits Protected Health Information on behalf of Business Associate.

6.4 If neither cure nor termination as set forth in Sections 6.2 and 6.3 is feasible, Business Associate shall immediately notify County.

6.5 Without limiting the requirements of Section 6.1, the agreement required by Section 6.1 (Subcontractor Business Associate Agreement) shall require Subcontractor to contemporaneously notify Covered Entity in the event of a Breach of Unsecured Protected Health Information.

6.6 Without limiting the requirements of Section 6.1, agreement required by Section 6.1 (Subcontractor Business Associate Agreement) shall include a provision requiring Subcontractor to destroy, or in the alternative to return

to Business Associate, any Protected Health Information created, received, maintained, or transmitted by Subcontractor on behalf of Business Associate so as to enable Business Associate to comply with the provisions of Section 18.4.

6.7 Business Associate shall provide to Covered Entity, at Covered Entity's request, a copy of any and all Subcontractor Business Associate Agreements required by Section 6.1.

6.8 Sections 6.1 and 6.7 are not intended by the parties to limit in any way the scope of Business Associate's obligations related to Subcontracts or Subcontracting in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

7. ACCESS TO PROTECTED HEALTH INFORMATION

7.1 To the extent Covered Entity determines that Protected Health Information is maintained by Business Associate or its agents or Subcontractors in a Designated Record Set, Business Associate shall, within two (2) business days after receipt of a request from Covered Entity, make the Protected Health Information specified by Covered Entity available to the Individual(s) identified by Covered Entity as being entitled to access and shall provide such Individuals(s) or other person(s) designated by Covered Entity with a copy the specified Protected Health Information, in order for Covered Entity to meet the requirements of 45 C.F.R. § 164.524.

7.2 If any Individual requests access to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate shall be referred to Covered Entity in writing within two (2) business days of the receipt of the request. Whether access shall be provided or denied shall be determined by Covered Entity.

7.3 To the extent that Business Associate maintains Protected Health Information that is subject to access as set forth above in one or more Designated Record Sets electronically and if the Individual requests an electronic copy of such information, Business Associate shall assist Covered Entity as reasonably necessary in providing the Individual with access to the Protected Health Information in the electronic form and format requested by the Individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by Covered Entity and the Individual.

8. AMENDMENT OF PROTECTED HEALTH INFORMATION

8.1 To the extent Covered Entity determines that any Protected Health Information is maintained by Business Associate or its agents or Subcontractors in a Designated Record Set, Business Associate shall, within ten (10) business days after receipt of a written request from Covered Entity, make any amendments to such Protected Health Information that are requested by Covered Entity, in order for Covered Entity to meet the requirements of 45 C.F.R. § 164.526.

8.2 If any Individual requests an amendment to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the receipt of the request. Whether an amendment shall be granted or denied shall be determined by Covered Entity. Covered Entity shall be responsible for responding to the Individual making the amendment request and for making any necessary corrections to that Individual's Protected Health Information.

9. ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

9.1 Business Associate shall maintain an accounting of each Disclosure of Protected Health Information made by Business Associate or its employees, agents, representatives or Subcontractors, as is determined by Covered Entity to be necessary in order to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

9.1.1 Any accounting of disclosures provided by Business Associate under Section 9.1 shall include:

(a) The date of the Disclosure;

(b) The name, and address if known, of the entity or person who received the Protected Health Information;

(c) A brief description of the Protected Health Information Disclosed; and

(d) A brief statement of the purpose of the Disclosure.

9.1.2 For each Disclosure that could require an accounting under Section 9.1, Business Associate shall document the information specified in Section 9.1.1, and shall maintain the information for six (6) years from the date of the Disclosure.

9.2 Business Associate shall provide to Covered Entity, within ten (10) business days after receipt of a written request from Covered Entity, information collected in accordance with Section 9.1.1 to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528

9.3 If any Individual requests an accounting of disclosures directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the receipt of the request, and shall provide the requested accounting of disclosures to the Individual(s) within 30 days. The information provided in the accounting shall be in accordance with 45 C.F.R. § 164.528.

10. COMPLIANCE WITH APPLICABLE HIPAA RULES

10.1 To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity's performance of such obligation(s).

10.2 Business Associate shall comply with all HIPAA Rules applicable to Business Associate in the performance of Services.

11. AVAILABILITY OF RECORDS

11.1 Business Associate shall make its internal practices, books, and records relating to the Use and Disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity available to the Secretary for purposes of determining Covered Entity's compliance with the Privacy and Security Regulations.

11.2 Unless prohibited by the Secretary, Business Associate shall immediately notify Covered Entity of any requests made by the Secretary and provide Covered Entity with copies of any documents produced in response to such request.

12. MITIGATION OF HARMFUL EFFECTS

12.1 Business Associate shall mitigate, to the extent practicable, any harmful effect of a Use or Disclosure of Protected Health Information by Business Associate in violation of the requirements of this Business Associate Agreement that is known to Business Associate.

13. BREACH NOTIFICATION TO INDIVIDUALS

In the event of a Breach of Unsecured Protected Health Information caused by Business Associate, its employees, representatives, agents or Subcontractors, Business Associate will provide the following information to Covered Entity:

(a) A brief description of what happened, including the date of the Breach and the date of the Discovery of the Breach, if known;
(b) A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
(c) Any steps the Individual should take to protect him or herself from potential harm resulting from the Breach;
(d) A brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individual(s), and to protect against any further Breaches; and
(e) Contact procedures for Individual(s) to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

13.2 Covered Entity will provide any required notification to individuals whose Unsecured Protected Health Information has been, or is reasonably believed to have been, accessed, acquired, Used, or Disclosed as a result of any such Breach, and Business Associate will assist as needed, as reasonably required by Covered Entity.

13.3 Business Associate shall reimburse Covered Entity for up to $9 million in costs incurred by Covered Entity, in complying with Subpart D of 45 C.F.R. Part 164, including but not limited to costs of notification, internet posting, or media publication, as a result of Business Associate's Breach of Unsecured Protected Health Information.

14. OBLIGATIONS OF COVERED ENTITY

14.1 Covered Entity shall notify Business Associate of any current or future restrictions or limitations on the Use or Disclosure of Protected Health Information that would affect Business Associate's performance of the Services, and Business Associate shall thereafter restrict or limit its own Uses and Disclosures accordingly.

14.2 Covered Entity shall not request Business Associate to Use or Disclose Protected Health Information in any manner that would not be permissible

under Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except to the extent that Business Associate may Use or Disclose Protected Health Information as provided in Sections 2.3, 2.5, and 2.6.

15. TERM

15.1 Unless sooner terminated as set forth in Section 16, the term of this Business Associate Agreement shall be the same as the term of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

15.2 Notwithstanding Section 15.1, Business Associate's obligations under Sections 11 and 17 shall survive the termination or expiration of this Business Associate Agreement.

16. TERMINATION FOR CAUSE

16.1 In addition to and notwithstanding the termination provisions set forth in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, if either party determines that the other party has violated a material term of this Business Associate Agreement, and the breaching party has not cured the breach or ended the violation within the time specified by the non-breaching party, which shall be reasonable given the nature of the breach and/or violation, the non-breaching party may terminate this Business Associate Agreement.

16.2 In addition to and notwithstanding the termination provisions set forth in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, if either party determines that the other party has violated a material term of this Business Associate Agreement, and cure is not feasible, the non-breaching party may terminate this Business Associate Agreement immediately.

17. DISPOSITION OF PROTECTED HEALTH INFORMATION UPON TERMINATION OR EXPIRATION

17.1 Except as provided in Section 17.3, upon termination for any reason or expiration of this Business Associate Agreement, Business Associate shall return or, if agreed to by Covered entity, shall destroy as provided for in Section 17.2, all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of

Covered Entity, that Business Associate, including any Subcontractor, still maintains in any form. Business Associate shall retain no copies of the Protected Health Information.

17.2 Destruction for purposes of Section 17.2 and Section 6.6 shall mean that media on which the Protected Health Information is stored or recorded has been destroyed and/or electronic media have been cleared, purged, or destroyed in accordance with the use of a technology or methodology specified by the Secretary in guidance for rendering Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals.

17.3 Notwithstanding Section 11.1, in the event that return or destruction of Protected Health Information is not feasible or Business Associate determines that any such Protected Health Information is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities, Business Associate may retain that Protected Health Information for which destruction or return is infeasible or that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities and shall return or destroy all other Protected Health Information.

17.3.1 Business Associate shall extend the protections of this Business Associate Agreement to such Protected Health Information, including continuing to use appropriate safeguards and continuing to comply with Subpart C of 45 C.F.R Part 164 with respect to Electronic Protected Health Information, to prevent the Use or Disclosure of such information other than as provided for in Sections 2.5 and 2.6 for so long as such Protected Health Information is retained, and Business Associate shall not Use or Disclose such Protected Health Information other than for the purposes for which such Protected Health Information was retained.

17.3.2 Business Associate shall return or, if agreed to by Covered entity, destroy the Protected Health Information retained by Business Associate when it is no longer needed by Business Associate for Business Associate's proper management and administration or to carry out its legal responsibilities.

17.4 Business Associate shall ensure that all Protected Health Information created, maintained, or received by Subcontractors is returned or, if agreed to by Covered entity, destroyed as provided for in Section 17.2.

18. AUDIT, INSPECTION, AND EXAMINATION

18.1 Covered Entity reserves the right to conduct a reasonable inspection of the applicable books, records, agreements, and policies and procedures

relating to the Use or Disclosure of Protected Health Information for the purpose determining whether Business Associate is in compliance with the terms of this Business Associate Agreement and any non-compliance may be a basis for termination of this Business Associate Agreement and the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, as provided for in section 16.

18.2 Covered Entity and Business Associate shall mutually agree in advance upon the scope, timing, and location of any such inspection.

18.3 At Business Associate's request, and to the extent permitted by law, Covered Entity shall execute a nondisclosure agreement, upon terms and conditions mutually agreed to by the parties.

18.4 That Covered Entity inspects, fails to inspect, or has the right to inspect as provided for in Section 18.1 does not relieve Business Associate of its responsibility to comply with this Business Associate Agreement and/or the HIPAA Rules or impose on Covered Entity any responsibility for Business Associate's compliance with any applicable HIPAA Rules.

18.5 Covered Entity's failure to detect, its detection but failure to notify Business Associate, or its detection but failure to require remediation by Business Associate of an unsatisfactory practice by Business Associate, shall not constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under this Business Associate Agreement or the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

18.6 Section 18.1 is not intended by the parties to limit in any way the scope of Business Associate's obligations related to Inspection and/or Audit and/or similar review in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

19. MISCELLANEOUS PROVISIONS

19.1 Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with the terms and conditions of this Business Associate Agreement will be adequate or satisfactory to meet the business needs or legal obligations of Business Associate.

19.2 HIPAA Requirements. The Parties agree that the provisions under HIPAA Rules that are required by law to be incorporated into this Amendment are hereby incorporated into this Agreement.

19.3 No Third Party Beneficiaries. Nothing in this Business Associate Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

19.4 Construction. In the event that a provision of this Business Associate Agreement is contrary to a provision of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, the provision of this Business Associate Agreement shall control. Otherwise, this Business Associate Agreement shall be construed under, and in accordance with, the terms of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

19.5 Regulatory References. A reference in this Business Associate Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

19.6 Interpretation. Any ambiguity in this Business Associate Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Rules.

19.7 Amendment. The parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the HIPAA Rules and any other privacy laws governing Protected Health Information.

BUSINESS ASSOCIATE LISTING

Business Associate Name:_____

Type of Services Provided:_____

Website URL:_____

First Point of Contact:

Title:_____

Name:_____

Address:_____

Phone:_____ **Fax:**_____**E-mail:**_____

Second Point of Contact:

Title:_____

Name:_____

Address:_____

Phone:_____ **Fax:**_____**E-mail:**_____

EXHIBIT M

INFORMATION SECURITY REQUIREMENTS

(ADDED UNDER AMENDMENT NUMBER TWELVE)

SEPTEMBER 2023

TRAUMA AND EMERGENCY MEDICINE INFORMATION SYSTEMS AGREEMENT

EXHIBIT M – INFORMATION SECURITY REQUIREMENTS

This Exhibit M (Information Security Requirements) is an attachment and addition to the Agreement, and is incorporated into the Agreement by reference hereof. Unless specifically defined in this Exhibit, capitalized terms shall have the meanings set forth in the Agreement.

1.1 INTRODUCTION

This Exhibit M (Information Security Requirements) sets forth the information security procedures and policies to be established by CONTRACTOR before the effective date of the Agreement and maintained throughout the Agreement Term. This Exhibit M (Information Security Requirements) is in addition to the other requirements of the Agreement, including Business Associate under the Health Insurance Portability and Accountability Act of 1996, between the parties, and presents a minimum standard only. It is CONTRACTOR's sole obligation to (i) implement appropriate measures to secure its systems and data against internal and external threats and risks to COUNTY confidential information; and (ii) continuously review and revise those measures to address ongoing threats and risks. Failure to materially comply with the minimum standards set forth in this Exhibit M (Information Security Requirements) will constitute a material, breach of the Agreement by CONTRACTOR, entitling COUNTY, in addition to and cumulative of all other remedies available to it at law, in equity, or under the Agreement, to immediately terminate the Agreement.

1.2 INFORMATION MANAGEMENT PROGRAMS

A. Security Program

The CONTRACTOR shall establish and maintain formal, documented, mandated, company-wide security programs, including security policies, standards and procedures (collectively, "Security Program").

"Confidentiality/Integrity/Availability" shall mean data, objects, and resources are protected from unauthorized viewing and other access; data is protected from unauthorized changes to ensure that it is reliable and correct; and authorized users have access to the systems and the resources they need.

The Security Program shall, at a minimum:

1. Protect the Confidentiality/Integrity/Availability of COUNTY Confidential Information accessed by CONTRACTOR or in the CONTRACTOR's possession or control.

2. Protect against any anticipated threats or hazards to the Confidentiality/Integrity/Availability of COUNTY Confidential Information.

3. Protect against unauthorized or unlawful access, use, disclosure, modification, or destruction of COUNTY Confidential Information.

4. Protect against accidental loss or destruction of, or damage to, COUNTY Confidential Information.

5. Safeguard COUNTY Confidential Information in compliance with any applicable laws and regulations which apply to the COUNTY and CONTRACTOR.

B. Privacy Program

The CONTRACTOR shall establish and maintain a company-wide program designed to incorporate policies and practices in its business operations to provide safeguards for sensitive and confidential information encountered in CONTRACTOR's operations, including the COUNTY Confidential Information (collectively, "Privacy Program"). Notwithstanding the foregoing, CONTRACTOR's Privacy Program shall solely relate to its practices, which may include handling of customer information, but shall not bind the COUNTY (including, but not limited to, its users, patients, and constituents) to CONTRACTOR's policies.

The CONTRACTOR's Privacy Program shall include:

1. A framework that identifies and ensures that the CONTRACTOR complies with all applicable laws and regulations.

2. A framework that supports ethical decision-making in product and service design or deployment that optimizes

3. A framework that supports ethical decision-making in product and service design or deployment that optimizes

beneficial uses of data while minimizing adverse consequences for individuals' privacy.

3. External and internal policies, procedures and controls to support the privacy program.

4. A training program that covers the foregoing policies, protocols and awareness.

5. A response plan to address incidents.

B. CONTRACTOR Personnel Training

The CONTRACTOR shall supply CONTRACTOR personnel with appropriate, annual training regarding information security procedures, risks, threats, and the Information Management Programs.

C. Storage and Transmission of COUNTY Confidential Information

All COUNTY Confidential Information shall be rendered unusable, unreadable, or indecipherable to unauthorized individuals. Without limiting the generality of the foregoing, the CONTRACTOR will encrypt all workstations, portable devices (e.g., mobile, wearables, tablets,) and removable data storage media (e.g., portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) ("Removable Media") that store COUNTY Confidential Information in accordance with Federal Information Processing Standard (FIPS) 140-2.

The CONTRACTOR will encrypt COUNTY Confidential Information transmitted on networks outside of the CONTRACTOR's control with Transport Layer Security (TLS) 1.2 or higher or Internet Protocol Security (IPSEC), at a minimum Cipher Strength of 128 bit.

All mobile devices storing COUNTY Confidential Information shall be managed by a mobile device management system which allows CONTRACTOR to control, secure, and enforce policies on smartphones, tablets, and other endpoints. Such system must provide provisions to enforce a password/passcode on enrolled mobile devices. All workstations/personal computers (including laptops, 2-in-1s, and tablets) will maintain current operating system security patches, and the latest virus definitions. Virus scans must be performed at least monthly.

D. Destruction of COUNTY Confidential Information

The CONTRACTOR shall return or destroy COUNTY Confidential Information in accordance with the Agreement. In the case of destruction, the CONTRACTOR shall destroy all originals and copies by (i) cross-cut shredding paper, film, or other hard copy media so that the information cannot be read or otherwise reconstructed; and (ii) purging, or destroying electronic media containing COUNTY Confidential Information consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization" or any successor standard such that the COUNTY Confidential Information cannot be retrieved. As to COUNTY Confidential Information in the possession or control of CONTRACTOR, the CONTRACTOR will provide an attestation on company letterhead and certified documentation from a media destruction firm, detailing the destruction method used and the COUNTY Confidential Information involved, the date of destruction, and the company or individual who performed the destruction. Such statement will be sent to COUNTY within ten (10) days of termination or expiration of the Agreement or at any time upon the COUNTY's request. As to COUNTY Confidential Information that is in the possession or control of an authorized Subprocessor, CONTRACTOR shall request destruction of the COUNTY Confidential Information and Subprocessor shall purge or destroy such COUNTY Confidential Information consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization" or any successor standard such that the COUNTY Confidential Information cannot be retrieved.

E. Physical and Environmental Security

The CONTRACTOR will implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the Confidentiality/Integrity/Availability of COUNTY Confidential Information.

F. Operational Management

The CONTRACTOR shall: (i) monitor and manage all of its information processing facilities, including, without limitation, implementing operational procedures, change management, and incident (as defined below) response procedures consistent with Paragraph I (Incidents); and (ii) deploy adequate anti-malware software and adequate back-up systems to ensure essential business information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures are

adequately documented and designed to protect information and computer media, and data from theft and unauthorized access.

G. Access Control

Subject to and without limiting the requirements under Paragraph D (Storage and Transmission of COUNTY Confidential Information), COUNTY Confidential Information (i) may only be made available and accessible to those parties explicitly authorized under the Agreement (including CONTRACTOR's employees who have a legitimated need), those who have been granted access by the COUNTY, or otherwise expressly approved by the COUNTY Project Director or Project Manager; (ii) if transferred across the internet, any wireless network (e.g., cellular, 802.11x, or similar technology), or other public or shared networks, must be protected using appropriate encryption technology as designated or approved by COUNTY in writing; and (iii) if transferred using removable media must be sent via a bonded courier and protected using encryption technology designated by the CONTRACTOR and approved by the COUNTY Chief Information Security Officer. The foregoing requirements shall also apply to back-up data stored by the CONTRACTOR at off-site facilities.

The CONTRACTOR shall implement formal procedures to control access to COUNTY systems, services, data, and/or information, including, but not limited to, user account management procedures and the following controls:

3. Network access to both internal and external networked services shall be controlled, including, but not limited to, the use of industry standard and properly configured firewalls.

4. Appropriate access controls will be applied to computer resources including, but not limited to, multi-factor authentication, use of virtual private networks (VPN), authorization, and event logging.

5. The CONTRACTOR will conduct regular, no less often than semi-annually, user access reviews to ensure that unnecessary and/or unused access to COUNTY Confidential Information is removed in a timely manner.

6. Applications will include access control to limit user access to COUNTY Confidential Information and application system functions.

7. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. The CONTRACTOR shall record, review and act upon all events in accordance with incident (as defined below) response policies set forth in Paragraph I (Incidents).

8. In the event any hardware, storage media, or removable media (as described in Paragraph D (Storage and Transmission of COUNTY Confidential Information) must be disposed of or sent off-site for servicing, the CONTRACTOR shall ensure all COUNTY Confidential Information, has been eradicated from such hardware and/or media using the standards in Paragraph E (Destruction of COUNTY Confidential Information).

H. Incidents

In the event of an Incident (as defined below), the CONTRACTOR shall:

3. Promptly notify the COUNTY's Chief Information Security Officer, the Departmental Information Security Officer, and the COUNTY's Chief Privacy Officer of any attempted or successful unauthorized access, use, disclosure, modification, destruction, sharing, application, examination, analysis, release, transfer, or divulging in any other manner (whether oral, electronic, or in writing) of COUNTY Confidential Information ("Incident"), within twenty-four (24) hours of detection of the Incident. All notifications shall be submitted via encrypted email and telephone.

COUNTY Chief Information Security Officer and Chief Privacy Officer Email:
Ciso-cpo_notify@laCOUNTY.gov

Chief Information Security Officer:
Jeffrey Aguilar
Chief Information Security Officer
320 W Temple, 7th floor
Los Angeles, CA 90012
(213) 253-5600

Chief Privacy Officer:
Lillian Russell

Chief Privacy Officer
320 W Temple, 7th floor
Los Angeles, CA 90012
(213) 351-5363

Departmental Information Security Officer Email:
Ehd@dhs.laCOUNTY.gov and
helpdesksup@dhs.laCOUNTY.gov
Vahe Haratounian
Department of Health Services Information Security Officer
Health Services Administration
313 North Figueroa, Suite 317
Los Angeles, CA 90012
(323) 409-8000

4. Include the following information:

   a. The date and time of discovery of the incident.

   b. The approximate date and time of the incident.

   c. A description of the type of COUNTY confidential information involved in the incident.

   d. A summary of the relevant facts, including a description of measures being taken to respond to and remediate the incident, and any planned corrective actions as they are identified.

   e. The name and contact information for the CONTRACTOR's official representative(s), with relevant business and technical information relating to the incident.

5. Cooperate with the COUNTY to investigate the Incident and seek to identify the specific COUNTY Confidential Information involved in the incident upon the COUNTY's written request, without charge, unless the Incident was caused by the acts or omissions of the COUNTY. As information about the incident is collected or otherwise becomes available to the CONTRACTOR, and unless prohibited by law, the CONTRACTOR shall provide information regarding the nature and consequences of the Incident that are reasonably requested by the COUNTY to allow the COUNTY to notify affected individuals, government agencies, and/or credit bureaus.

6. Promptly initiate the appropriate portions of their Business Continuity and/or Disaster Recovery plans in the event of an Incident causing a material interference with COUNTY's information technology operations.

7. Assist and cooperate with forensic investigators, the COUNTY, law firms, and and/or law enforcement agencies to help determine the nature, extent, and source of any incident, and reasonably assist and cooperate with the COUNTY on any additional disclosures that the COUNTY is required to make as a result of the Incident.

Subject to the limits of the Limitation of Liability in Paragraph 102 (SaaS Limitation of Liability), the CONTRACTOR shall be (i) liable for all damages and fines, (ii) responsible for all CONTRACTOR corrective action and payment for the reasonable costs of COUNTY's corrective action, and (iii) responsible for, at COUNTY's sole election, all notifications arising from an incident or COUNTY's reasonable costs for such notifications, caused by or arising from the CONTRACTOR's weaknesses, negligence, errors, lack of information security or privacy controls or provisions, or CONTRACTOR's failure to comply with the applicable terms under this Exhibit M (Information Security Requirements) and otherwise under the Agreement.

I. Audit and Inspection

3. Self-Audits

a. The CONTRACTOR shall periodically conduct audits, assessments, testing of the system of controls, and testing of information security and privacy procedures, including penetration testing, intrusion detection, and firewall configuration reviews. These periodic audits will be conducted by staff certified to perform the specific audit in question at CONTRACTOR's sole cost and expense through either (i) an internal independent audit function, or (ii) a nationally recognized, external, independent auditor.

b. The CONTRACTOR shall have a process for correcting control deficiencies that have been identified in the periodic audit, including follow up documentation providing evidence of such corrections. Failure to correct or obviate control deficiencies within a commercially reasonable period of time shall constitute a material breach of the Agreement. The

CONTRACTOR shall provide a high level summary of the audit results and any corrective action documentation to the COUNTY promptly upon its completion at the COUNTY's request. With respect to any other report, certification, or audit or test results prepared or received by the CONTRACTOR that contains any COUNTY Confidential Information, the CONTRACTOR shall promptly provide the COUNTY with copies of the same upon the COUNTY's reasonable request, including identification of any failure or exception in the CONTRACTOR's information systems, products, and services, and the corresponding steps taken by the CONTRACTOR to mitigate such failure or exception. Any reports and related materials provided to the COUNTY pursuant to this Paragraph J (Audit and Inspection) shall be provided at no additional charge to the COUNTY and treated as confidential information by the COUNTY.

4. COUNTY Audits

a. At its own expense, the COUNTY, or an independent third-party auditor commissioned by the COUNTY, shall have the right to audit the CONTRACTOR's infrastructure, security and privacy practices, data center, services and/or systems storing or processing COUNTY Confidential Information via an onsite inspection at least once a year or more frequently upon reasonably suspected violation of this Exhibit M (Information Security Requirements), provided COUNTY and CONTRACTOR will agree in advance to the parameters of such audit, and COUNTY and its independent third-party auditor executes appropriate confidentiality agreements with Contractor. Such audit shall be conducted during the CONTRACTOR's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect the CONTRACTOR's normal business operations. The COUNTY's request for the audit will specify the scope and areas (e.g., administrative, physical, and technical) that are subject to the audit and may include, but is not limited to physical controls inspection, process reviews, policy reviews, evidence of external and internal vulnerability scans, penetration test results, evidence of code reviews, and evidence of system

configuration and audit log reviews. It is understood that the results may be filtered to remove the specific information of other CONTRACTOR customers such as IP address, server names, etc. The CONTRACTOR shall cooperate with the COUNTY in the development of the scope and methodology for the audit, and the timing and implementation of the audit. This right of access shall extend to any regulators with oversight of the COUNTY. The CONTRACTOR agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes. Upon the COUNTY's request, the CONTRACTOR shall complete a questionnaire regarding CONTRACTOR's information security practices and/or program. When not prohibited by law, the CONTRACTOR will provide to the COUNTY a summary of: (i) the results of any security audits, security reviews, or other relevant audits, conducted by the CONTRACTOR or a third party related to the systems used to provide services to COUNTY; and (ii) corrective actions or modifications, if any, the CONTRACTOR will implement in response to such audits.

b. When not prohibited by law, the CONTRACTOR will notify the COUNTY if CONTRACTOR's privacy or security practices related to the systems used to provide services to COUNTY are investigated or audited by any federal or state regulatory body. Such notification shall consist of the details of the audit or investigation, and the CONTRACTOR's corrective actions with respect to any deficiencies that were identified in the audit or investigation.