

DigitalEMS Subscription Agreement



SUBSCRIPTION AGREEMENT

This **Medic ClipBoard** Subscription Agreement (the "Agreement") is made and entered into on September 16, 2025, by and between DigitalEMS Solutions Incorporated ("DigitalEMS"), a California corporation and the **City of Redondo Beach** ("Customer"), a chartered municipal corporation.

1. **Medic ClipBoard.** ("System")

- 1.1. Licensed Software.** The licensed software is the *Medic ClipBoard* system, a system comprising of multiple parts: an iOS (Apple's mobile operating system) application ("Front-End") that performs reporting of patient information, a web-based administrative support back-end ("Back-End") that performs data collection, analysis, and reporting over the Internet (the "Licensed Software") for the Emergency Medical Services (EMS) industry. DigitalEMS Solutions Inc. owns all the rights to this software.
- 1.2. Professional Services.** DigitalEMS makes available many professional services ("Professional Services") per Section 4 to help maximize your investment in DigitalEMS. Services include, but may not be limited to, Application Support, Classroom Training, Educational Resources, and Custom Programming to the System.
- 1.3. System Integration Services.** DigitalEMS integrates the System with many third-party systems, such as CAD (Computer-Aided-Dispatch), medical devices, billing, and local reporting systems. These integration services may be provided on a fee-for-services basis or may be included in the Subscription Fees, and/or evaluated on a case-by-case basis.
- 1.4. Data Collection Services.** DigitalEMS provides the System as a flexible data collection solution for the Customer using the proprietary electronic Patient Care Report ("ePCR") using mobile hardware and a secure file transfer that uploads data via the Internet (the "Data Collection Services"). Certain Data Collection Services require the Customer to procure and support hardware that meets the specifications set forth by DigitalEMS.
- 1.5. Data Center Services.** The Data Center ("Data Center") is comprised of infrastructure and services that host, manage, and support the System. DigitalEMS is responsible for the Data Center as defined in Section 5.2 up to the point of external Internet access. It is the responsibility of the Customer to procure applicable hardware, software, and Internet Connectivity with sufficient bandwidth to meet the user demands. DigitalEMS uses a third party Business Associate to handle the Data Center and hardware that support the Back-End part of the System. DigitalEMS will do its due diligence to uphold this Agreement as defined herein.

2. INITIAL SETUP

- 2.1. Customer's Responsibilities for Setup.** Customer must provide Internet connectivity to the System with sufficient bandwidth to meet the Customer's utilization demands. System performance is a function of bandwidth and latency time from client hardware to the System. Customer must connect to Back-End with a web browser that will support the latest web technologies (e.g., HTML5).
- 2.2. Customer Passwords.** Both a login identity and a password are necessary to access the System Back- End through a web browser. The password provides a vital security in preventing unauthorized access to the Customer's Data and Confidential Information. DigitalEMS shall require each user to authenticate via unique credentials, consisting of a site-specific code, username, and a password, which shall be a minimum of 12 characters, including at least one uppercase letter, one lowercase letter, one digit, and one special character. Customer is responsible for keeping and maintaining the security of the passwords that are assigned to the Customers employees. DigitalEMS shall have no responsibility for the unauthorized access to the Customer's Data or Confidential Information that results from the Customers failure to keep the assigned passwords secure.

- 2.3. System Activation Date.** The System Activation Date (“Activation Date”) is defined in Schedule P. The System Activation Date is the date at which DigitalEMS will activate the System to allow for Customer set-up of the Licensed Software via the Data Center.
- 2.4. System Go-Live Date.** The System Go-Live Date (“Go-Live”) is defined in Schedule P. The Go-Live date is the date at which the Customer has properly set up their Back-End, the Customers employees have been trained in the use of the System, and the Customer is ready for live field use of the System.

3. LICENSE AND FEES

- 3.1. License.** DigitalEMS hereby grants the Customer a non-exclusive, non-transferable, license to access the System on their iOS hardware and over the Internet, based on the payment of the Customer’s subscription fees as set forth in Schedule P.
- 3.2. Fees.**
- 3.2.1. System Set-Up Fees.** System Set-Up Fees are the one-time per Provider Initial System Activation and Provider Set-up as set forth on Schedule P.
- 3.2.2. Subscription Fees.** Customer agrees to pay Subscription Fees as set forth on Schedule P, which forms a part of this Subscription Agreement. Fees include: Data Center Services, Data Collection Services, Application Licensing, System Maintenance, and Application Support. System Upgrades are the sole prerogative of DigitalEMS.
- 3.2.3. Invoicing.** Following the identification of Customer’s System Go Live Date as set forth in Schedule P, DigitalEMS will invoice the Customer for Subscription Fees as defined in the Schedule P.
- 3.2.4. Payment.** Payment for services rendered under this Agreement shall be due within 60 calendar days from Customer’s receipt of invoice. The fee schedule and rates are as set forth on Schedule P, which forms a part of this Subscription Agreement. In the event of non- payment, Digital EMS retains the right to terminate system access to the Customer. DigitalEMS will provide a minimum of a thirty calendar day notification when terminating system access. If services are terminated by either party, any outstanding payments for services rendered up to the termination date shall be due within 60 calendar days of the receipt of the termination notice.
- 3.2.5. Taxes.** Currently, electronic software is exempt from sales tax under IRC Section 108. However, if this section is amended, DigitalEMS may be required to collect sales tax from products and services provided to customers in the state of California. DigitalEMS reserves the right to invoice the Customer those taxes that are imposed by any governmental authority upon the sale or delivery of items purchased or licensed. Customer shall be held harmless by DigitalEMS from penalties or accruing interest for failure of DigitalEMS to pay sales tax.

4. PROFESSIONAL SERVICES

- 4.1. Application Support.** DigitalEMS provides phone and email Application Support of the System at no additional cost to Customers who have completed Train-the-Trainer Classroom Training and are active Users. Application support is defined as help with application navigation or troubleshooting arising from the use of the System, as designed. DigitalEMS’s phone support will provide unlimited Customer support during the hours of 8:00 am - 5:00 pm PST. After-hour System support consists of a voice-messaging system in which the Customer will be required to leave a message containing a brief synopsis of the issue, and a contact name and number. It is DigitalEMS’s goal to return after-hour messages within one hour of receiving them or first thing in the morning for late night calls. As to avoid many calls from the Customer’s employees, the Customer will designate one to five employees who will act as the point of contact between DigitalEMS and the Customer. Application Support excludes supporting Customer procured hardware, OS and Internet connectivity.
- 4.2. Classroom Training.** DigitalEMS offers training regarding the use of the System for the benefit of its Customers. Training will be offered at the rate defined in Schedule P. Should the Customer, at a later date, require additional Training, it will be the Customer’s responsibility to pay for the requested additional training.

4.3. Custom Programming. If the Customer desires to have the System perform in a way that is not already included in the System, this will require DigitalEMS to perform Custom Programming ("Custom Programming"). The Customer will provide DigitalEMS with an outlined requirement of such Custom Programming requirements. Digital EMS shall provide a detailed scope of work and fixed pricing after DigitalEMS has assessed the necessary Custom Programming time required to complete such requirements. DigitalEMS will not begin work on the said Custom Programming until the Customer has agreed to enter into a Software Development Agreement ("SDA") with DigitalEMS. DigitalEMS will charge the Customer at the standard rate as defined below. The SDA is not included within this Agreement, and is a separate Agreement that the Customer will enter into with DigitalEMS should the Customer request Custom Programming to be done by DigitalEMS.

4.3.1. Developer's Services. DigitalEMS shall provide to Customer professional services in the area of software development, human user interface design, graphic design, web page design, application design and development, mobile device application design or development, project management, testing & QA, research or any other consulting, development, management, software or graphic services. All services will be executed remotely. No on-site work or travel shall be performed.

- **HOURLY RATE.** In consideration of the Services to be performed by Developer under this Agreement, Customer will pay Developer for time spent on Services, at the following rates:

\$125 per hour Web Development, \$150 per hour Mobile Development

5. DATA CENTER SERVICES

5.1. System Maintenance. DigitalEMS will provide software upgrades and system enhancements when DigitalEMS determines the upgrades are essential for the Customer. DigitalEMS will coordinate the installation of software upgrades and system enhancements for Customer at no charge to the Customer. Should DigitalEMS decide that upgrades or enhancements to the System are needed, DigitalEMS will notify the Customer one week in advance if the said upgrade or enhancement will cause an interruption to any part of the System. If the said upgrade or enhancement is to be made to the Front-End, explicit instructions will be sent to the Customer on how to do the said upgrade or enhancement as to minimize impact to the Customer's business activity.

5.2. System Access Level.

5.2.1. DigitalEMS shall take all commercially reasonable steps to ensure the integrity, security, and availability of Customer data. Any interruption in service or loss of data attributable to DigitalEMS's failure to comply with the backup and failover protocols set forth in this Agreement shall result in full liability on the part of DigitalEMS, including but not limited to the obligation to restore the affected data and provide a pro-rata refund of the Customer's subscription fees for the period during which the interruption or loss occurred.

5.2.2. DigitalEMS shall maintain a level of access to the Data Center (excluding periods of scheduled or emergency maintenance) of 99.8% Access Availability ("Access Availability"), 24 hours a day, 7 days a week, including holidays. System Access Unavailable ("System Access Unavailable") is defined as the reported unscheduled inability of users of the Customer to access the Data Center and verification that the problem is within the Data Center. DigitalEMS shall utilize Amazon Web Services (AWS) for hosting, and shall implement automated nightly, weekly, and monthly backups, with real-time replication through AWS's Multi-AZ redundancy feature. In the event of a failure, AWS will automatically switch to a standby database server to ensure data continuity and integrity. Backup data shall be retained for a period of fourteen (14) days.

5.2.3. DigitalEMS is not responsible for loss of access to the Data Center for reasons that are beyond DigitalEMS's reasonable control, such as acts of war, terrorism, natural disasters, government actions, power outages, and third-party telecommunication failures, provided that DigitalEMS has adhered to all backup and failover obligations.

5.2.4. If DigitalEMS fails to meet its obligations under this Agreement due to its negligence or willful

misconduct, DigitalEMS shall be responsible only for the direct damages arising from such failure, subject to the liability limitations set forth in Section 11.3. In no event shall DigitalEMS be liable for any consequential, incidental, indirect, or special damages, and the total liability for all claims under this Section shall not exceed the subscription fees paid by the Customer to DigitalEMS in the twelve (12) months preceding the event giving rise to the claim, as provided in Section 11.3. Any additional compensatory services, such as credits, as reasonably required by Customer, shall be provided at no charge.

6. TERM AND TERMINATION

- 6.1. Term Initiation.** This agreement takes effect on the latest signature date below and continues through the conclusion of the Subscription Term or any subsequent renewed Subscription Terms. The Subscription Term (the “Term”) begins on the System Activation Date and ends at the conclusion of the period set forth in Schedule P or any subsequent renewed Subscription Terms. Subscription Fees commence on the System Activation Date and continue throughout the Term of this Agreement. Upon acceptance of this Agreement, DigitalEMS will provide Customer with the appropriate login credentials to use the Licensed Software via DigitalEMS’s Data Center and the Internet.
- 6.2. Term Renewal.** This agreement may be renewed upon such terms and for such period set forth in a new Schedule P (the “Renewal Schedule P”) provided by DigitalEMS and executed by Customer within thirty (30) days before the end of the then current Term. If Customer does not execute the Renewal Schedule P, this agreement shall automatically terminate upon expiration of the then current Term. When the conclusion of the period as set forth in Schedule P is nearing ninety (90) days from the Term conclusion, DigitalEMS will issue a Renewal Schedule P to the Customer.
- 6.3. Termination.**
- 6.3.1 Termination for Breach.** Either party may terminate the Agreement upon the other party’s material breach of this Agreement, if within 45 days of receipt of written notification of breach, the breaching party has failed to cure its breach. DigitalEMS may terminate Customer’s access to the System immediately upon Termination of the Agreement. In the event of early Termination due to material breach by the Customer, Customer will be responsible for Early Termination Fee per Section 6.4 of this Agreement.
- 6.3.2 Termination for Convenience.** Additionally, Customer may terminate this Agreement and Customer obligations hereunder during the initial Term or any subsequent renewal Term, without cause, for any reason, or for no reason, and in Customer’s sole and absolute discretion. Customer must notify DigitalEMS of its intention for early Termination by written notification at least 30 days before the desired Termination date. In such an event, DigitalEMS shall ensure that any data uploaded to the system prorated at the standard rate as stipulated on Schedule P, and any remaining balance will be refunded to the Customer within 30 days of Customer’s written request of such refund. No Early Termination Fee applies under Section 6.3.2.
- 6.3.3 Material Breach.** For the purposes of this Agreement, “Material Breach” means a breach of this Agreement that: (i) results in a failure to perform any of the following obligations – data security, confidentiality of PHI under Section 10, timely delivery of Services, or payment of Fees; or (ii) otherwise causes a substantial and demonstrable harm to the non-breaching party, such as exposure of PHI. A breach that is minor, technical, or promptly cured, and that does not materially impair such benefits, shall not constitute a Material Breach
- 6.4. Early Termination Fee (Only for Material Breach by Customer).** Customer agrees to pay all fees as stipulated on the Schedule P on an annual basis throughout the term of the Agreement. Upon early Termination of the Agreement, all records uploaded to the system will be prorated at the standard fee as stipulated on Schedule P and any remaining balance will be refunded to the Customer.
- 6.5. Data Ownership and Retrieval.** All data generated through the use of the System is solely the property of the Customer. Upon termination or expiration of the Agreement, DigitalEMS shall return all Customer data in a digital format. This will include, but is not limited to, PDFs, incident JSON data, and in any editable format

specified by the Customer (e.g., CSV, JSON, XLS, XLSX, etc.), to facilitate smooth migration to another solution. DigitalEMS will securely destroy all copies of the Customer's data stored in its systems within thirty days of receiving Customer's written request, except for any data that must be retained by law. Upon completion of the data destruction, DigitalEMS shall provide the Customer with a written certification confirming the destruction and specifying the methods used.

- 6.6. Remedies.** If Customer attempts to use, copy, license, sub-license or otherwise transfer the Licensed Software or access to the System supplied by DigitalEMS under this Agreement, in a manner contrary to the terms of this Agreement or in competition with DigitalEMS or in derogation of DigitalEMS's proprietary rights, whether these rights are explicitly stated, determined by law, or otherwise, DigitalEMS shall have the right to injunctive relief enjoining such action, in addition to any other remedies available. Customer acknowledges that other remedies are inadequate.
- 6.7. Infringement Indemnification.** DigitalEMS shall indemnify, defend and hold harmless Customer from and against any and all lost, cost, damage, or liability, including reasonable attorneys' fees and expenses, arising out of or relating to any claim or cause of action for patent, copyright, and/or other intellectual property infringement. ("Infringement Claim") asserted against Customer by virtue of the System, Software or Documentation or Customer's use of possession of the System, Software or Documentation pursuant to this agreement. DigitalEMS shall defend and settle at its sole expense all suits and proceedings arising out of the foregoing, providing that Customer gives DigitalEMS prompt written notice of any such Infringement Claim of which it learns. In all events, Customer shall have the right to participate at its own expense in the defense of any such suit or proceeding through counsel of its own choosing. In the event any Infringement Claim is asserted by a third party with respect to the System or Customer's use thereof, then and in that event, Customer may terminate its use of the System and/or this Agreement without payment of any Early Termination Fee.

7. PROPRIETARY RIGHTS OF DIGITALEMS IN THE LICENSED SOFTWARE

- 7.1. Nature of Rights and Title.** Customer acknowledges that the System and System documentation manuals and other proprietary information, materials supplied by DigitalEMS to Customer are and shall remain the property of DigitalEMS and nothing in this Agreement shall be construed as transferring any aspect of such Customer or any third party. Any changes, additions, and enhancements in the form of a new or partial programs or documentation as may be provided under this Agreement shall remain the proprietary property of DigitalEMS. Customer agrees with DigitalEMS that the System documentation and all other proprietary information or data supplied by DigitalEMS are trade secrets of DigitalEMS, are protected by criminal and civil law, and by the law of copyright, are valuable to DigitalEMS, and that their use and disclosure must be carefully and continuously controlled. Customer shall keep each and every item to which DigitalEMS retains title free and clear of all claims, liens, and encumbrances except those of DigitalEMS and any act of Customer, voluntary or involuntary, purporting to create a claim, lien or encumbrance on such an item shall be void.
- 7.2. Unauthorized Acts.** Customer agrees to notify DigitalEMS promptly of the unauthorized possession, use, or knowledge of any item supplied under this license and of other information made available to Customer under this Agreement, by any person or organization not authorized by this Agreement to have such possession, use, or knowledge. Customer will promptly furnish full details of such possession, use or knowledge to DigitalEMS, will assist in preventing the continuation or recurrence of such possession, use or knowledge, and will cooperate with DigitalEMS in any litigation against third parties deemed necessary by DigitalEMS to protect its proprietary rights. Customer's compliance with this subparagraph shall not be construed in any way as waiver to DigitalEMS's right, if any, to recover damages or obtain other relief against Customer for its negligent or intentional harm to DigitalEMS's proprietary rights, or for breach of contractual rights.

8. LIMITED WARRANTY

- 8.1. Software.** For the duration of this Agreement (the "Warranty Period"), DigitalEMS will checkout, document

and deliver any amendments or alterations to the License Software that may be required to correct errors which significantly effect performance. This warranty is contingent upon the Customer advising DigitalEMS in writing of such errors. DigitalEMS shall not be responsible for maintaining Customer-modified portions of the License Software. Corrections for difficulties or defects traceable to Customer errors or System changes will be billed at the standard DigitalEMS time and materials rates.

THE LIMITED WARRANTY SET FORTH IN THE AGREEMENT IS THE ONLY WARRANTY MADE BY DIGITALEMS. DIGITALEMS EXPRESSLY DISCLAIMS, AND CUSTOMER HERBY EXPRESSLY WAIVES, ALL OTHER WARRANTIES EXPRESS, IMPLIED OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE. DIGITALEMS DOES NOT WARRANT THAT THE LICENSED SOFTWARE WILL MEET CUSTOMER'S REQUIREMENTS OR THAT THE OPERATION OF THE LICENSED SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT, EXCEPT AS REQUIRED HEREIN TO ADDRESS ERRORS THAT SIGNIFICANTLY EFFECT PERFORMANCE, ERRORS IN THE LICENSE SOFTWARE WILL BE CORRECTED. DIGITALEMS'S LIMITED WARRANTY IS IN LIEU OF ALL LIABILITIES OR OBLIGATIONS OF DIGITALEMS FOR THE DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE INSTALLATION, USE OR PERFORMANCE OF THE SYSTEM.

9. DATA

- 9.1. Use.** Customer grants DigitalEMS a perpetual, royalty-free license to compile, analyze, and use de-identified aggregated data derived from information obtained through the Customer's use of the System during the Term. This data will be used solely to understand how the system is utilized and to make improvements. The data remains the property of the Customer, and upon termination of this Agreement, data handling shall be governed by Section 6.5. DigitalEMS represents and warrants that it will employ methods to de-identify the data that ensure no actual disclosure or Protected Health Information is accessible to DigitalEMS.
- 9.2. Backups.** Customer's **full** data will be backed up on a daily basis with a fourteen (14) day retention of said backup. DigitalEMS will maintain the copy of the **full** backup for a period of fourteen (14) days at which time it will be deleted to ensure space for the following fourteen (14) days of backup data. Customer's backup(s) will be maintained on a rolling basis and DigitalEMS will not be responsible for archiving more than the most recent fourteen (14) days of **full** backup data. DigitalEMS will take commercially reasonable steps to maintain data integrity of any backup, but DigitalEMS is not responsible for loss of data or data integrity so long as DigitalEMS has performed the backup in a commercially reasonable manner.
- 9.3. Data Migration.** As Customer migrates from its current electronic patient reporting system, World Advancement of Technology for EMS and Rescue (WaterOnScene), to DigitalEMS, both parties agree to coordinate the migration of data to the DigitalEMS system.
- DigitalEMS shall seamlessly integrate Customer's previous data into the DigitalEMS system. DigitalEMS acknowledges that the data from WaterOnScene was transitioned from the Trauma and Emergency Medicine Information System (TEMIS) to the National Emergency Medical Services Information System (NEMSIS) version 3.4/3.5. Consequently, DigitalEMS cannot guarantee that all data fields will match on a 1:1 basis with the DigitalEMS system, but will make every effort to perform the most accurate integration possible. DigitalEMS shall store the original files obtained from WaterOnScene for a period of two years to troubleshoot and reimport incidents which have not migrated successfully. Copies of incidents which are unable to migrate successfully after this period shall be provided to Customer.
 - DigitalEMS will set a maximum cap of 25 hours for the integration process, billed at the hourly rates specified in Schedule P (not to exceed a total cost of \$5,000)
 - Should additional hours be required beyond this cap, DigitalEMS and Customer will negotiate in good faith a mutually agreed upon amendment to this Agreement. to complete the integration. If no agreement is reached within 45 days, either party may terminate the migration services without

penalty, and DigitalEMS shall provide a prorated refund for any unused portion of the capped hours, while ensuring partial data migration is delivered in a usable format to the Customer.

10. BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Business Associate Agreement"), effective as of Activation Date, is entered into by and between DigitalEMS ("Business Associate") and Customer (the "Covered Entity") to ensure that DigitalEMS Solutions, Inc. will appropriately safeguard Protected Health Information ("PHI") that is created, received, maintained, or transmitted on behalf of the Covered Entity in compliance with the applicable provisions of Public Law 104-191 of August 21, 1996, known as the Health Insurance Portability and Accountability Act of 1996, Subtitle F – Administrative Simplification, Sections 261, et seq., as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, Title XII, Subtitle D – Privacy, of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, and as may be amended from time to time, and regulations promulgated thereunder, (collectively "HIPAA"). The terms of this Section 10 constitute the full Business Associate Agreement between the parties hereto and shall prevail over any conflicting provisions in the Agreement regarding PHI.

10.1. DEFINITIONS

- 10.1.1. Business Associate. "Business Associate" shall mean DigitalEMS.
- 10.1.2. Covered Entity. "Covered Entity" shall mean Customer.
- 10.1.3. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
- 10.1.4. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
- 10.1.5. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- 10.1.6. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.103.
- 10.1.7. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee

10.2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

- 10.2.1 Business Associate shall not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law. No use or disclosure for any purpose beyond those specifically outlined is permitted without prior written authorization from the Covered Entity.
- 10.2.2 Business Associate shall use the following safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Agreement. Business Associate shall implement and maintain appropriate safeguards to protect the confidentiality, integrity, and availability of PHI, including:
 - Encryption: PHI must be encrypted using AES-256 or another industry-standard encryption protocol, both in transit and at rest, with no exceptions.
 - Access Controls: Business Associate shall ensure that access to PHI is strictly limited to authorized personnel and shall use multi-factor authentication and role-based access control.
 - Employee Background Checks: All personnel with access to PHI must undergo a comprehensive background check to ensure they do not pose a security risk.
 - Annual Training: All personnel of Business Associate with access to PHI shall complete

- annual HIPAA and cybersecurity training.
 - Data Destruction: Upon termination of this Agreement or when PHI is no longer required, Business Associate shall irreversibly destroy all PHI in compliance with NIST standards.
- 10.2.3 Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by the Agreement of which it becomes aware, including breaches of unsecured PHI as required at 45 CFR 164.410, and any security incident as defined under 45 CFR 164.304. This includes the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI, or interference with system operations in an information system. Business Associate shall notify Covered Entity within seventy-two (72) hours of discovering any breach of security incident of which it becomes aware. Notification shall include detailed information regarding the breach, including the nature and scope of the breach, the types of PHI involved, and the steps taken to mitigate any potential harm.
- 10.2.4 Business Associate agrees to ensure that in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information, including compliance with all cybersecurity measures and encryption requirements.
- 10.2.5 Business Associate shall make PHI available to the Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 CFR §164.524 within 15 days of Covered Entity's request.
- 10.2.6 Business Associate shall submit any amendment(s) to PHI in a designated record set as directed or agreed to by Covered Entity pursuant to 45 CFR 164.526 within 15 days, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526.
- 10.2.7 Business Associate agrees to maintain and provide accounting of disclosures to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528 within 30 days of request.
- 10.2.8 Business Associate agrees to the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation(s); and
- 10.2.9 Business Associate agrees to make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA.
- 10.2.10 Business Associate shall establish and maintain ongoing audit and monitoring processes to ensure compliance with this Agreement. Any unauthorized access attempts must be immediately reported to the Covered Entity.
- 10.2.11 Business Associate shall provide to Covered Entity, at least annually and upon request, a written certification of its compliance with this Business Associate Agreement and applicable HIPAA requirements including verification that all required safeguards (e.g., encryption, access controls) are implemented and effective.
- 10.2.12 Business Associate shall comply with additional state laws, such as the California Confidentiality Medical Information Act (Cal. Civ. Code § 56 et seq.)

10.3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

- 10.3.1. Business Associate may only use or disclose PHI only as permitted or required by this Agreement or as required by law. No use or disclosure for any purpose beyond those specifically outlined is permitted without prior written authorization from the Covered Entity.
- 10.3.2. Business Associate may use or disclose PHI for the proper management and administration of its own business only to the extent required by law.
- 10.3.3. Business Associate agrees to make uses and disclosures and requests PHI in compliance with Covered Entity's minimum necessary policies and procedures.
- 10.3.4. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity, except for the specific uses and disclosures set forth below.
- 10.3.5. Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.
- 10.3.6. Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided the disclosures are

required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

- 10.3.7. Business Associate may provide data aggregation services relating to the health care operations of the Covered Entity, provided such services are explicitly permitted under this Agreement.

10.4. OBLIGATIONS OF COVERED ENTITY

- 10.4.1. Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
- 10.4.2. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
- 10.4.3. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

10.5. PERMISSIBLE REQUESTS BY COVERED ENTITY

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 CFR Part 164 if done by covered entity. An exception is if the Business Associate will use or disclose protected health information for, data aggregation or management and administrative activities of Business Associate.

10.6. TERM AND TERMINATION

- 10.6.1. **Term.** The Term of this Agreement shall be effective as of Activation Date, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

- 10.6.2. **Termination for Cause.** Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

- 10.6.2.1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
- 10.6.2.2. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or
- 10.6.2.3. If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

10.6.3. Effect of Termination

- 10.6.3.1 Upon termination or expiration of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health

Information.

10.6.3.2 In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon sixty (60) days that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

10.7 MISCELLANEOUS

- 10.7.1 Regulatory References.** A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.
- 10.7.2 Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
- 10.7.3 Survival.** The respective rights and obligations of Business Associate under Section 10 of this Agreement shall survive the termination of this Agreement.
- 10.7.4 Interpretation.** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

11. INDEMNIFICATION

11.1 In addition to other specific indemnification obligations outlined in this Agreement, including but not limited to Section 6.7, DigitalEMS shall indemnify, defend, and hold harmless the Customer, its elected official, officers, employees, agents, and contractors (collectively "Indemnitees") from and against any and all liabilities, claims, damages, losses, fines, penalties, judgments, costs, and expenses, including but not limited to, reasonable attorneys' fees and expenses to the extent directly caused by DigitalEMS's

- (a) material breach of this Agreement;
- (b) gross negligence or willful misconduct; or
- (c) violation of applicable laws in connection with the performance of this Agreement.

11.2 Specific Indemnification Scenarios. Subject to the limitations in this Section:

- (a) **Breach of Contract.** Any direct losses arising from DigitalEMS's material breach of its obligations under this Agreement.
- (b) **HIPAA and Data Privacy Violations.** Any violation of HIPAA or related privacy laws caused by DigitalEMS's gross negligence, willful misconduct, or failure to comply with Section 10.
- (c) **Data Breaches and Cybersecurity Failures.** Any unauthorized access, disclosure, or **destruction** of data caused by DigitalEMS's gross negligence or willful misconduct, and only to the extent such breach is attributable to DigitalEMS.
- (d) **Third-Party Claims.** Any third-party claim arising directly from DigitalEMS's failure to perform its obligations under this Agreement, except to the extent such claim is caused by the other Party or a third party completely outside DigitalEMS's control.
- (e) **Gross Negligence and Misconduct.** Any direct losses caused by the DigitalEMS's gross negligence or willful misconduct.
- (f) **Intellectual Property Infringement.** Intellectual property infringement claims are addressed exclusively under Section 6.7 of this Agreement.
- (g) **Regulatory Fines and Penalties.** Any fines, penalties, or costs imposed by regulatory authorities arising from DigitalEMS's non-compliance with this Agreement.

11.3 Limitations on Liability.

- (a) DigitalEMS will not be liable for any consequential, incidental, indirect, special, or punitive damages, regardless of the theory of liability. This limitation does not apply to claims arising from gross negligence, willful misconduct, HIPAA violations, data breaches, or intellectual property infringement; provided that damages for any such claims are recoverable only as provided in Section 11.3(b) of this Agreement.
- (b) The total cumulative liability of DigitalEMS under this Section shall not exceed the total subscription fees paid by the Customer to DigitalEMS in the twelve (12) months preceding the event giving rise to the claim, except that this limitation shall not apply to claims arising from gross negligence, willful misconduct, HIPAA violations, data breaches, intellectual property infringement, or regulatory fines and penalties, where liability shall be capped at the limits outlined in DigitalEMS's attached insurance requirements described in Section 12 of this Agreement.

11.4 Procedure. The Customer shall:

- (a) promptly notify DigitalEMS in writing of any claim for which indemnification is sought;
- (b) permit DigitalEMS to control the defense and settlement of such claim, provided that any settlement fully releases the Customer from all liability and does not impose any admission of fault or ongoing obligation without the prior written consent of the Customer (which shall not be unreasonably withheld); and
- (c) reasonably cooperate in the defense at the DigitalEMS's expense.

12. INSURANCE

DigitalEMS shall comply with the insurance requirements, attached hereto and incorporated herein.

13. GENERAL

Section 13 sometimes refers to DigitalEMS and Customer as each a "Party" and collectively the "Parties".

- 13.1. Amendment.** This Agreement can only be modified by a written agreement duly signed by persons authorized to sign agreements on behalf of Customer and of DigitalEMS, and variance from the terms and conditions of this Agreement in any order or other written notification from the Customer will be of no effect.
- 13.2. Severability.** If any provision or provisions of this Agreement shall be held to be invalid, illegal or unenforceable, the validity, legality, and enforceability of the remaining provisions shall not in any way be affected or impaired thereby.
- 13.3. Applicable Law.** This Agreement shall, in all respects, be interpreted, construed, and governed by and under the domestic laws of the State of California. Any judicial or arbitral proceedings brought to interpret or enforce this Agreement shall be brought in the County of Los Angeles, State of California.
- 13.4. Incorporation by Reference.** This Agreement incorporates by reference the following documents, which are attached hereto and made a part hereof:
 - 13.4.1. Schedule P. Fee schedule and implementation dates.
 - 13.4.2. Statement of Work ("SOW"). Detailed description of the services to be provided by DigitalEMS.
- 13.5. Entirety of Agreement.** DigitalEMS and Customer hereto acknowledge and agree that this Agreement, and other instruments (including Schedule P and the Statement of Work) specifically referred to herein, if any, constitute and contain the entire Agreement and understanding concerning the subject matter between DigitalEMS and Customer and supersede and replace all prior negotiations and proposed agreements, whether written or oral. Each of the parties warrants that no other party or any agent or attorney of any other party has made any promise, representations, or warranty whatsoever not contained herein to induce it to execute the Agreement and the other documents referred to herein, if any. Each of the Parties represents that they have not executed this Agreement in reliance on any promise, representation, or warranty whatsoever not contained herein, to induce them to execute this Agreement and the other documents referred to herein, if any. Each of the Parties represents that he has not executed this

Agreement or the other documents, if any, in reliance on any promise, representation, or warranty not contained herein.

- 13.6. Conflict Resolution.** In the event of any conflict or inconsistency between the terms of this Agreement, Schedule, P, and the SOW, the terms of this Agreement shall govern and control. For the avoidance of doubt, the order of hierarchy shall apply: (i) the terms of this Agreement (including the Business Associate Agreement in Section 10, which prevails on all matters related to PHI); (ii) the Insurance Requirements; (iii) SOW; and (iv) Schedule P.
- 13.7. Headings.** The various headings used in this Agreement are inserted for convenience only, and do not vary the meaning of the Agreement.
- 13.8. Signature.** This Agreement may be executed in counterparts, and any signature evidenced by facsimile or scanned and emailed shall have the same validity as an original ink signature.

[SIGNATURES FOLLOW ON NEXT PAGE]

IN WITNESS HEREOF, DigitalEMS Solutions Inc. and Customer shall execute this Agreement by their signatures listed herein below.

CITY OF REDONDO BEACH,
a chartered municipal corporation

James A. Light, Mayor

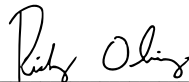
ATTEST:

Eleanor Manzano, City Clerk

APPROVED AS TO FORM:

Joy A. Ford, City Attorney

DIGITALEMS SOLUTIONS, INC.,
a California corporation


Ricky Olivarez, CEO

DigitalEMS Solutions, Inc.
34 Savona Walk
Long Beach, CA 90803
Tax Payer ID: 27-2674189

APPROVED:

Diane Strickfaden, Risk Ma

INSURANCE REQUIREMENTS

Without limiting DigitalEMS's indemnification obligations under this Agreement, DigitalEMS shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder by the DigitalEMS, its agents, representatives, or employees.

Minimum Scope of Insurance

Coverage shall be at least as broad as:

Insurance Services Office Commercial General Liability coverage (occurrence form CG 0001).

Insurance Services Office form number CA 0001 (Ed. 1/87) covering Automobile Liability, code 1 (any auto).

Cyber Liability Insurance.

Minimum Limits of Insurance

DigitalEMS shall maintain limits no less than:

General Liability: \$2,000,000 per occurrence for bodily injury, personal injury and property damage. The general aggregate limit shall apply separately to this project.

Automobile Liability: \$1,000,000 per accident for bodily injury and property damage.

Cyber Liability Insurance: \$3,000,000 per occurrence for data breaches, cyberattacks, and other cybersecurity risks.

Deductibles and Self-Insured Retentions

Any deductibles or self-insured retentions must be declared to and approved by the Customer. At the option of the Customer, either: (1) the insurer shall reduce or eliminate such deductibles or self-insured retentions as respects the Customer, its officers, officials, employees and volunteers or (2) the DigitalEMS shall provide a financial guarantee satisfactory to the Customer guaranteeing payment of losses and related investigations, claim administration and defense expenses.

Other Insurance Provisions

The general liability and automobile liability policies are to contain, or be endorsed to contain, the following provisions:

Additional Insured Endorsement:

General Liability: The Customer, its officers, elected and appointed officials, employees, and volunteers shall be covered as insureds with respect to liability arising out of work performed by or on behalf of the DigitalEMS. General liability coverage can be provided in the form of an endorsement to the DigitalEMS's insurance, or as a separate owner's policy.

Automobile Liability: The Customer, its officers, elected and appointed officials, employees, and volunteers shall be covered as insureds with respect to liability arising out of automobiles owned, leased, hired or borrowed by or on behalf of the DigitalEMS.

Cyber Liability: The Customer, its officers, elected and appointed officials, employees, and volunteers shall be covered as insureds with respect to liability for data breaches, cyberattacks, and other cybersecurity risks. Cyber Liability coverage can be provided in the form of an endorsement to the DigitalEMS's insurance, or as a separate owner's policy.

For any claims related to this project, the DigitalEMS's insurance coverage shall be primary insurance as respects the Customer, its officers, elected and appointed officials, employees, and volunteers. Any insurance or self-insurance maintained by the Customer, its officers, officials, employees, or volunteers shall be excess of the DigitalEMS's insurance and shall not contribute with it.

Each insurance policy required by this clause shall be endorsed to state that coverage shall not be canceled by either party, except after thirty (30) days prior written notice by certified mail, return receipt requested, has been given to the Customer.

Each insurance policy shall be endorsed to state that the inclusion of more than one insured shall not operate to impair the rights of one insured against another insured, and the coverages afforded shall apply as though separate policies had been issued to each insured.

Each insurance policy shall be in effect prior to awarding the contract and each insurance policy or a successor policy shall be in effect for the duration of the project. The maintenance of proper insurance coverage is a material element of the contract and failure to maintain or renew coverage or to provide evidence of renewal may be treated by the Customer as a material breach of contract on the DigitalEMS's part.

Acceptability of Insurers

Insurance shall be placed with insurers with a current A.M. Best's rating of no less than A:VII and which are authorized to transact insurance business in the State of California by the Department of Insurance.

Verification of Coverage

DigitalEMS shall furnish the Customer with original certificates and amendatory endorsements effecting coverage required by this clause. The endorsements should be on the Customer authorized forms provided with the contract specifications. Standard ISO forms which shall be subject to Customer approval and amended to conform to the Customer's requirements may be acceptable in lieu of Customer authorized forms. All certificates and endorsements shall be received and approved by the Customer before the contract is awarded. The Customer reserves the right to require complete, certified copies of all required insurance policies, including endorsements effecting the coverage required by these specifications at any time.

Subcontractors

DigitalEMS shall include all subcontractors as insured under its policies or shall furnish separate certificates and endorsements for each subcontractor. All coverages for subcontractors shall be subject to all of the requirements stated herein.

Risk Management

DigitalEMS acknowledges that insurance underwriting standards and practices are subject to change, and the Customer reserves the right to make changes to these provisions in the reasonable discretion of its Risk Manager.