



Contract Number

SAP Number

Department of Public Health

| | |
|---|--|
| Department Contract Representative | <u>Michael Shin, Contract Analyst</u> |
| Telephone Number | <u>(909) 386-8146</u> |
| Contractor | <u>Insight Management Systems, Inc.</u> |
| Contractor Representative | <u>Shella Manansala</u> |
| Telephone Number | <u>(818) 385-0123 x.108</u> |
| Contract Term | <u>March 1, 2021 through February 28, 2026</u> |
| Original Contract Amount | <u>Not to Exceed \$17,000</u> |
| Amendment Amount | <u>N/A</u> |
| Total Contract Amount | <u>Not to Exceed \$17,000</u> |
| Cost Center | <u></u> |

IT IS HEREBY AGREED AS FOLLOWS:

WHEREAS, The County of San Bernardino, Department of Public Health (DPH), hereafter referred to as "County", desires license, maintenance and support of Omnicare software to enter and record data related to care coordination of children with health conditions that require diagnosis and treatment, including data reporting and follow up contact with families for appointments; and

WHEREAS, County has been allocated funds by the State to provide such services; and

WHEREAS, County finds Insight Management Systems, Inc., hereafter referred to as "Contractor", qualified to provide such services; and

WHEREAS, County desires that such services be provided by Contractor and Contractor agrees to perform these services as set forth below;

NOW THEREFORE, County and Contractor mutually agree to the following terms and conditions:

TABLE OF CONTENTS

| | |
|--|---|
| I. CONTRACTOR AND COUNTY RESPONSIBILITIES..... | 4 |
| II. CONTRACTOR GENERAL RESPONSIBILITIES..... | 4 |
| III. FISCAL PROVISIONS | 6 |
| IV. TERM..... | 7 |
| V. EARLY TERMINATION | 7 |
| VI. GENERAL PROVISIONS | 7 |
| VII. CONCLUSION..... | 9 |

ATTACHMENTS

ATTACHMENT A – BUSINESS ASSOCIATE AGREEMENT

ATTACHMENT B – ADDENDUM A TO BUSINESS ASSOCIATE AGREEMENT

ATTACHMENT C – BUSINESS ASSOCIATE ADDENDUM FOR CLOUD SERVICES

ATTACHMENT D – OMNICARE: ANNUAL LICENSE, MAINTENANCE and HIPAA BAA RENEWAL
INVOICE

ATTACHMENT E – INSIGHT MANAGEMENT SYSTEMS, INC. SOFTWARE and SERVICES - STANDARD
LICENSE AGREEMENT

I. CONTRACTOR AND COUNTY RESPONSIBILITIES

Contractor and County shall:

- A. Adhere to the terms and conditions of the attached Business Associate Agreement (Attachment A).
- B. Adhere to the terms and conditions of the attached Addendum A to Business Associate Agreement (Attachment B).
- C. Adhere to the terms and conditions of the attached Omnicare: Annual License, Maintenance and HIPAA BAA Renewal Invoice (Attachment C).
- D. Adhere to the terms and conditions of the attached Business Associate Addendum for Cloud Services – Software as a Service (Attachment D).
- E. Adhere to the terms and conditions of the attached Insight Management Systems, Inc. Software and Services – Standard License Agreement (Attachment E).

II. CONTRACTOR GENERAL RESPONSIBILITIES

- A. Without prior written consent of the County, this Contract is not assignable by Contractor either in whole or in part.
- B. Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, regulations have been promulgated governing the privacy of individually identifiable health information. Contractor acknowledges that it is a covered entity and subject to the requirements of HIPAA and HITECH, and their implementing regulations. The HIPAA Privacy Rule and Security Rule specify requirements with respect to contracts between a Covered Entity and its Business Associates. Contractor shall execute and comply with the attached Business Associate Agreement. Contractor further agrees to comply with the requirements of other federal and state law that applies to the information collected and maintained by Contractor for Services performed pursuant to Contract.
- C. To the extent applicable, if Contractor is a business that collects the personal information of a consumer(s) in performing Services pursuant to this Contract, Contractor must comply with the provisions of the California Consumer Privacy Act (CCPA) (Cal. Civil Code §§1798.100, et seq.). For purposes of this provision, “business,” “consumer,” and “personal information” shall have the same meanings as set forth at Civil Code Section 1798.140. Contractor must contact the County immediately upon receipt of any request by a consumer submitted pursuant to the CCPA that requires any action on the part of the County, including but not limited to, providing a list of disclosures or deleting personal information. Contractor must not sell, market or otherwise disclose personal information of a consumer provided by the County unless specifically authorized pursuant to terms of this Contract. Contractor must immediately provide to the County any notice provided by a consumer to Contractor pursuant to Civil Code section 1798.150(b) alleging a violation of the CCPA that involves personal information received or maintained pursuant to this Contract. Contractor must immediately notify the County if it receives a notice of violation from the California Attorney General pursuant to Civil Code section 1798.155(b).
- D. Contractor agrees to and shall comply with the following indemnification and insurance requirements:
 - 1. Indemnification – The Contractor agrees to indemnify, defend (with counsel reasonably approved by County) and hold harmless the County and its authorized officers, employees, agents and volunteers from any and all claims, actions, losses, damages, and/or liability arising out of this contract from any cause

whatsoever, including the acts, errors or omissions of any person and for any costs or expenses incurred by the County on account of any claim except where such indemnification is prohibited by law. This indemnification provision shall apply regardless of the existence or degree of fault of indemnitees. The Contractor's indemnification obligation applies to the County's "active" as well as "passive" negligence but does not apply to the County's "sole negligence" or "willful misconduct" within the meaning of Civil Code Section 2782. In addition, Contractor will indemnify, defend, and hold harmless County and its officers, employees, agents and volunteers, from any and all third party claims, costs (including without limitation reasonable attorneys' fees), and losses for infringement of any United States patent, copyright, trademark or trade secret (Intellectual Property Rights) by any goods or services. If a credible claim is made or threatened, including without limitation the filing of a lawsuit against County, or County receives a demand or notice claiming actual or potential infringement or misappropriation of any Intellectual Property Rights, County will use reasonable efforts to notify Contractor promptly of such lawsuit, claim or election. However, County's failure to provide or delay in providing such notice will relieve Contractor of its obligations only if and to the extent that such delay or failure materially prejudices Consultant's ability to defend such lawsuit or claim. County will give Contractor sole control of the defense (with counsel reasonably acceptable to County) and settlement of such claim; provided that Contractor may not settle the claim or suit absent the written consent of County unless such settlement (a) includes a release of all claims pending against County, (b) contains no admission of liability or wrongdoing by County, and (c) imposes no obligations upon County other than an obligation to stop using the goods or services that are the subject of the claim. In the event that Contractor fails to or elects not to defend County against any claim for which County is entitled to indemnity by Contractor, then Contractor shall reimburse County for all reasonable attorneys' fees and expenses within thirty (30) days from date of invoice or debit memo from County. After thirty (30) days, County will be entitled to deduct any unpaid invoice or debit memo amount from any amounts owed by County to Contractor. This shall not apply to any judgment or settlement amount, which amounts County shall be entitled to notify, invoice or debit Contractor's account at any time; and County, at its sole discretion, may settle the claim or suit.

If, in Contractor's opinion, any goods or services become, or are likely to become, the subject of a claim of infringement of Intellectual Property Rights, Contractor may, at its option: (i) procure for County the right to continue using the goods or receiving the services; (ii) replace or modify the goods or services to be non-infringing, without incurring a material diminution in performance or function; or (iii) if neither of the foregoing is feasible, in the reasonable judgment of Contractor, County shall cease use of the goods or services upon written notice from Contractor, and Contractor shall provide County with a pro-rata refund of the unearned fees paid by County to Contractor for such goods or services.

2. Additional Insured – All policies, except for Workers' Compensation, Errors and Omissions and Professional Liability policies, shall contain additional endorsements naming the County and its officers, employees, agents and volunteers as additional named insureds with respect to liabilities arising out of the performance of services hereunder. The additional insured endorsements shall not limit the scope of coverage for the County to vicarious liability but shall allow coverage for the County to the full extent provided by the policy. Such additional

insured coverage shall be at least as broad as Additional Insured (Form B) endorsement form ISO, CG 2010.1185.

3. Waiver of Subrogation Rights – The Contractor shall require the carriers of required coverages to waive all rights of subrogation against the County, its officers, employees, agents, volunteers, contractors and subcontractors. All general or auto liability insurance coverage provided shall not prohibit the Contractor and Contractor's employees or agents from waiving the right of subrogation prior to a loss or claim. The Contractor hereby waives all rights of subrogation against the County.
4. Policies Primary and Non-Contributory – All policies required herein are to be primary and non-contributory with any insurance or self-insurance programs carried or administered by the County.
5. Severability of Interests – The Contractor agrees to ensure that coverage provided to meet these requirements is applicable separately to each insured and there will be no cross liability exclusions that preclude coverage for suits between the Contractor and the County or between the County and any other insured or additional insured under the policy.
6. Proof of Coverage – The Contractor shall furnish Certificates of Insurance to the County Department administering the Contract evidencing the insurance coverage at the time the Contract is executed, additional endorsements, as required, shall be provided prior to the commencement of performance of services hereunder, which certificates shall provide that such insurance shall not be terminated or expire without thirty (30) days written notice to the Department, and Contractor shall maintain such insurance from the time Contractor commences performance of services hereunder until the completion of such services. Within fifteen (15) days of the commencement of this Contract, the Contractor shall furnish a copy of the Declaration page for all applicable policies and will provide complete certified copies of the policies and endorsements immediately upon request.
7. Acceptability of Insurance Carrier – Unless otherwise approved by Risk Management, insurance shall be written by insurers authorized to do business in the State of California and with a minimum "Best" Insurance Guide rating of "A-VII".
8. Deductibles and Self-Insured Retention – Any and all deductibles or self-insured retentions in excess of \$10,000 shall be declared to and approved by Risk Management.
9. Failure to Procure Coverage – In the event that any policy of insurance required under this Contract does not comply with the requirements, is not procured, or is canceled and not replaced, the County has the right but not the obligation or duty to cancel the Contract or obtain insurance if it deems necessary and any premiums paid by the County will be promptly reimbursed by the Contractor or County payments to the Contractor will be reduced to pay for County purchased insurance.
10. Insurance Review – Insurance requirements are subject to periodic review by the County. The Director of Risk Management or designee is authorized, but not required, to reduce, waive or suspend any insurance requirements whenever Risk Management determines that any of the required insurance is not available, is unreasonably priced, or is not needed to protect the interests of the County. In addition, if the Department of Risk Management determines that heretofore unreasonably priced or unavailable types of insurance coverage or coverage limits

become reasonably priced or available, the Director of Risk Management or designee is authorized, but not required, to change the above insurance requirements to require additional types of insurance coverage or higher coverage limits, provided that any such change is reasonable in light of past claims against the County, inflation, or any other item reasonably related to the County's risk.

Any change requiring additional types of insurance coverage or higher coverage limits must be made by amendment to this Contract. Contractor agrees to execute any such amendment within thirty (30) days of receipt.

Any failure, actual or alleged, on the part of the County to monitor or enforce compliance with any of the insurance and indemnification requirements will not be deemed as a waiver of any rights on the part of the County.

11. The Contractor agrees to provide insurance set forth in accordance with the requirements herein. If the Contractor uses existing coverage to comply with these requirements and that coverage does not meet the specified requirements, the Contractor agrees to amend, supplement or endorse the existing coverage to do so. The type(s) of insurance required is determined by the scope of the contract services.

Without in anyway affecting the indemnity herein provided and in addition thereto, the Contractor shall secure and maintain throughout the contract term the following types of insurance with limits as shown:

- a. Workers' Compensation/Employer's Liability – A program of Workers' Compensation insurance or a state-approved, self-insurance program in an amount and form to meet all applicable requirements of the Labor Code of the State of California, including Employer's Liability with \$250,000 limits covering all persons including volunteers providing services on behalf of the Contractor and all risks to such persons under this Contract.

If Contractor has no employees, it may certify or warrant to the County that it does not currently have any employees or individuals who are defined as "employees" under the Labor Code and the requirement for Workers' Compensation coverage will be waived by the County's Director of Risk Management.

With respect to Contractors that are non-profit corporations organized under California or Federal law, volunteers for such entities are required to be covered by Workers' Compensation insurance.

- b. Commercial/General Liability Insurance – The Contractor shall carry General Liability Insurance covering all operations performed by or on behalf of the Contractor providing coverage for bodily injury and property damage with a combined single limit of not less than one million dollars (\$1,000,000), per occurrence. The policy coverage shall include:

1. Premises operations and mobile equipment.
2. Products and completed operations.
3. Broad form property damage (including completed operations).
4. Explosion, collapse and underground hazards.
5. Personal injury.
6. Contractual liability.

7. \$2,000,000 general aggregate limit.

- c. Automobile Liability Insurance – Primary insurance coverage shall be written on ISO Business Auto coverage form for all owned, hired and non-owned automobiles or symbol 1 (any auto). The policy shall have a combined single limit of not less than one million dollars (\$1,000,000) for bodily injury and property damage, per occurrence.

If the Contractor is transporting one (1) or more non-employee passengers in performance of contract services, the automobile liability policy shall have a combined single limit of two million dollars (\$2,000,000) for bodily injury and property damage per occurrence.

If the Contractor owns no autos, a non-owned auto endorsement to the General Liability policy described above is acceptable.

- d. Umbrella Liability Insurance – An umbrella (over primary) or excess policy may be used to comply with limits or other primary coverage requirements. When used, the umbrella policy shall apply to bodily injury/property damage, personal injury/advertising injury and shall include a “dropdown” provision providing primary coverage for any liability not covered by the primary policy. The coverage shall also apply to automobile liability.

- e. Professional Liability – Professional Liability Insurance with limits of not less than one million (\$1,000,000) per claim and two million (\$2,000,000) aggregate limits.

or

Errors and Omissions Liability Insurance with limits of not less than one million (\$1,000,000) and two million (\$2,000,000) aggregate limits.

or

Directors and Officers Insurance coverage with limits of not less than one million (\$1,000,000) shall be required for contracts with charter labor committees or other not-for-profit organizations advising or acting on behalf of the County.

If insurance coverage is provided on a “claims made” policy, the “retroactive date” shall be shown and must be before the date of the start of the contract work. The claims made insurance shall be maintained or “tail” coverage provided for a minimum of five (5) years after contract completion.

- f. Cyber Liability Insurance – Cyber Liability Insurance with limits of no less than \$1,000,000 for each occurrence or event with an annual aggregate of \$2,000,000 covering privacy violations, information theft, damage to or destruction of electronic information, intentional and/or unintentional release of private information, alteration of electronic information, extortion and network security. The policy shall protect the involved County entities and cover breach response cost as well as regulatory fines and penalties.

- E. Contractor shall comply with all applicable laws, statutes, ordinances, administrative orders, rules or regulations relating to its duties, obligations and performance under the terms of the Contract and shall procure all licenses and pay all fees and other charges required thereby. Contractor shall maintain all required licenses during the term of this

Contract. Failure to comply with the provisions of this section may result in immediate termination of this Contract.

- F. If any legal action is instituted to enforce any party's rights hereunder, each party shall bear its own costs and attorney fees, regardless of who is the prevailing party. This paragraph shall not apply to those costs and attorney fees directly arising from a third-party legal action against a party hereto and payable under Indemnification and Insurance Requirements.

III. FISCAL PROVISIONS

- A. The maximum amount payment under this Contract shall not exceed \$17,000 of which \$[indicate federal dollars, if applicable] may be federally funded and shall be subject to availability of other funds to the County. The consideration to be paid to Contractor, as provided herein, shall be in full payment for all Contractor's services and expenses incurred in the performance hereof, including travel and per diem.
- B. Invoices shall be issued annually in the form of an Omnicare: Annual License, Maintenance and HIPAA BAA Renewal Invoice (Attachment E), with corresponding SAP Contract and/or Purchasing Order number stated on the invoice, and shall be processed within a net sixty (60) day payment term following approval by County.
- C. Contractor shall accept all payments from County via electronic funds transfer (EFT) directly deposited into the Contractor's designated checking or other bank account. Contractor shall promptly comply with directions and accurately complete forms provided by County required to process EFT payments.
- D. County is exempt from Federal excise taxes and no payment shall be made for any personal property taxes levied on Contractor or on any taxes levied on employee wages. The County shall only pay for any State or local sales or use taxes on the services rendered or equipment and/or parts supplied to the County pursuant to the contract.

IV. TERM

This Contract is effective as of March 1, 2021 and expires February 28, 2026, but may be terminated earlier in accordance with provisions of Section V of the Contract.

V. EARLY TERMINATION

- A. The County and the Contractor each reserve the right to terminate the Contract, for any reason, with a thirty (30) day written notice of termination. Such termination may include all or part of the services described herein.
- B. Upon such termination, payment will be made to the Contractor for services rendered and expenses reasonably incurred prior to the effective date of termination.
- C. Upon receipt of termination notice Contractor shall promptly discontinue services unless the notice directs otherwise. Contractor shall deliver promptly to County and transfer title (if necessary) all completed work, and work in progress, including drafts, documents, plans, forms, data, products, graphics, computer programs and reports.

VI. GENERAL PROVISIONS

- A. The Assistant Executive Officer for Human Services or his/her designee shall represent the County in all matters pertaining to the services to be rendered under this Contract, including termination and assignment of this Contract, and shall be the final authority in all matters pertaining to the Services/Scope of Work by Contractor. If this contract was initially approved by the San Bernardino County Board of Supervisors, then the Board of Supervisors must approve all amendments to this Contract.

- B. All written notices provided for in this Contract or which either party desires to give to the other shall be deemed fully given, when made in writing and either served personally, or by facsimile, or deposited in the United States mail, postage prepaid, and addressed to the other party as follows:

Contractor: Insight Management Systems, Inc.
17337 Ventura Blvd., #307
Encino, CA 91316

County: County of San Bernardino
Human Services
Attn: Contracts Unit
150 S. Lena Road
San Bernardino, CA 92415-0515

- C. In the event of any inconsistency between the terms of this Contract and any forms, attachments, statements of work (SOW), or specifications which may be incorporated into this Contract, the following order of precedence shall apply:

1. Applicable Federal and State laws, regulations and policies;
2. The Business Associate Agreement;
3. The terms and conditions in the body of this Contract;
4. the Terms of Exhibits, Attachments and/or other documents attached to this Contract, provided that no order of precedence shall be applied among such exhibits attachments and/or other documents, except the Business Associate Agreement; and
5. Price lists, SOWs, and other documents provided after execution of this Contract.

- D. Nothing contained in this Contract shall be construed as creating a joint venture, partnership or employment arrangement between the Parties hereto, nor shall either Party have the right, power or authority to create an obligation or duty, expressed or implied, on behalf of the other Party hereto.

- E. Failure by a party to insist upon the strict performance of any of the provisions of this Contract by the other party, or the failure by a party to exercise its rights upon the default of the other party, shall not constitute a waiver of such party's right to insist and demand strict compliance by the other party with the terms of this Contract thereafter.

- F. Any alterations, variations, modifications, or waivers of provisions of the Contract, unless specifically allowed in the Contract, shall be valid only when they have been reduced to writing, duly signed and approved by the Authorized Representatives of both parties as an amendment to this Contract. No oral understanding or agreement not incorporated herein shall be binding on any of the Parties hereto.

- G. If any provision of the Contract is held by a court of competent jurisdiction to be unenforceable or contrary to law, it shall be modified where practicable to the extent necessary so as to be enforceable (giving effect to the intention of the Parties) and the remaining provisions of the Contract shall not be affected.

- H. This Contract shall be governed by and construed in all aspects in accordance with the laws of the State of California without regard to principles of conflicts of laws. The parties acknowledge and agree that this Contract was entered into and intended to be performed in San Bernardino County, California. The parties agree that the venue of any action or claim brought by any party to this Contract will be the Superior Court of California, County of San Bernardino, San Bernardino District. Each party hereby waives any law or rule of

the court, which would allow them to request or demand a change of venue. If any action or claim concerning this Contract is brought by any third party and filed in another venue, the parties hereto agree to use their best efforts to obtain a change of venue to the Superior Court of California, County of San Bernardino, San Bernardino District.

- I. In the event the County determines that service is unsatisfactory, or in the event of any other dispute, claim, question or disagreement arising from or relating to this Contract or breach thereof, the parties hereto shall use their best efforts to settle the dispute, claim, question or disagreement. To this effect, they shall consult and negotiate with each other in good faith and, recognizing their mutual interests, attempt to reach a just and equitable solution satisfactory to both parties.
- J. The parties actions under the Contract shall comply with all applicable laws, rules, regulations, court orders and governmental agency orders. The provisions of this Contract are specifically made severable. If a provision of the Contract is terminated or held to be invalid, illegal or unenforceable, the validity and enforceability of the remaining provisions shall remain in full effect.
- K. In the event that a subpoena or other legal process commenced by a third party in any way concerning the services provided under this Contract is served upon Contractor or County, such party agrees to notify the other party in the most expeditious fashion possible following receipt of such subpoena or other legal process. Contractor and County further agree to cooperate with the other party in any lawful effort by such other party to contest the legal validity of such subpoena or other legal process commenced by a third party as may be reasonably required and at the expense of the party to whom the legal process is directed, except as otherwise proceed herein in connection with defense obligations by Contractor for County.
- L. This Contract supersedes and replaces all previous contracts, agreements and understandings, oral, written and implied, between the County and Contractor hereto with respect to the subject matter hereof. All such prior contracts, agreements and understandings are hereby terminated and deemed of no further force or effect.

VII. CONCLUSION

- A. This Contract, is the full and complete document describing services to be rendered by Contractor to County, including all covenants, conditions, and benefits.
- B. The signatures of the Parties affixed to this Contract affirm that they are duly authorized to commit and bind their respective institutions to the terms and conditions set forth in this document.
- C. This Contract may be executed in any number of counterparts, each of which so executed shall be deemed to be an original, and such counterparts shall together constitute one and the same Contract. The parties shall be entitled to sign and transmit an electronic signature of this Contract (whether by facsimile, PDF or other email transmission), which signature shall be binding on the party whose name is contained therein. Each party providing an electronic signature agrees to promptly execute and deliver to the other party an original signed Contract upon request.

IN WITNESS WHEREOF, the Board of Supervisors of the County of San Bernardino has caused this Contract to be subscribed to by the Clerk thereof, and Contractor has caused this Contract to be subscribed in its behalf by its duly authorized officers, the day, month, and year written.

COUNTY OF SAN BERNARDINO

►

Curt Hagman, Chairman

Dated: _____

SIGNED AND CERTIFIED THAT A COPY OF THIS
DOCUMENT HAS BEEN DELIVERED TO THE
CHAIRMAN OF THE BOARD

Lynna Monell
Clerk of the Board of Supervisors
of the County of San Bernardino

By _____

Deputy

Insight Management Systems, Inc.

(Print or type name of corporation, company, contractor, etc.)

By _____

(Authorized signature - sign in blue ink)

Name Shella Manansala

(Print or type name of person signing contract)

Title Administrator

(Print or Type)

Dated: _____

Address 17337 Ventura Boulevard, Suite 307

Encino, CA 91316

FOR COUNTY USE ONLY

Approved as to Legal Form

►

Bonnie Uphold, Deputy County Counsel

Date _____

Reviewed for Contract Compliance

►

Jennifer Mulhall-Daudel, Contracts Manager

Date _____

Reviewed/Approved by Department

►

Corwin Porter, Director

Date _____

BUSINESS ASSOCIATE AGREEMENT

Except as otherwise provided in this Agreement, Insight Management Systems, Inc. (IMS), hereinafter referred to as Business Associate, may use, access, maintain or disclose Protected Health Information to perform functions, activities or services for or on behalf of the County of San Bernardino, hereinafter referred to as the Covered Entity, as specified in this Agreement and the attached **CONTRACT**, provided such use, access, maintenance or disclosure does not violate the Health Insurance Portability and Accountability Act (HIPAA), 42 United States Code (USC) 1320d et seq., and its implementing regulations, including but not limited to, 45 Code of Federal Regulations (CFR) Parts 160, 162, and 164, hereinafter referred to as the "Privacy and Security Rules" and patient confidentiality regulations, including but not limited to, Title 42 of the Code of Federal Regulations Part 2 and the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), Public Law 111-5 (HITECH) and any regulations adopted or to be adopted pursuant to HITECH that relate to the obligations of business associates. Business Associate recognizes and agrees it is obligated by law to meet the applicable provisions of HITECH.

A. Definitions

- A. "Breach" means the acquisition, access, use or disclosure of Protected Health Information (PHI) in a manner not permitted under HIPAA (45 CFR Part 164, Subpart E), which compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a Breach unless the Covered Entity or Business Associate demonstrates that there is a low probability that the PHI has been compromised. A breach shall not include:
1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of Covered Entity or the Business Associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rules; or
 2. Any inadvertent disclosure by a person who is authorized to access PHI at Covered Entity or Business Associate to another person authorized to access Protected Health Information at Covered Entity or Business Associate, respectively, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; or
 3. A disclosure of PHI where Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- B. "Business Associate" means with respect to a Covered Entity, a person who:
1. On behalf of such Covered Entity, but other than in the capacity of a member of the workforce of such Covered Entity creates, receives, maintains or transmits PHI for a function or activity involving the use or disclosure of Personally Identifiable Health Information, including claims processing or administration, data analysis, data storage, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
 2. Provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for Covered Entity where the provision of the service involves the disclosure of PHI from such Covered Entity to the person.

A Covered Entity may be the Business Associate of another Covered Entity.

- C. “Covered Entity” means a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by the Privacy and Security Rules.
- D. “Data Aggregation” means, with respect to PHI created or received by a Business Associate in its capacity as the Business Associate of a Covered Entity, the combining of such PHI by the Business Associate with the PHI received by the Business Associate in its capacity as a Business Associate of another Covered Entity, to permit data analyses that relate to the health care operations of the respective Covered Entities.
- E. “Discovered” means a Breach shall be treated as discovered by Covered Entity or Business Associate as of the first day on which such Breach is known to such Covered Entity or Business Associate, respectively, (including any person, other than the individual committing the Breach, that is an employee, officer or other agent of such entity or associate, respectively) or should reasonably have been known to such Covered Entity or Business Associate (or person) to have occurred.
- F. “Electronic Protected Health Information” or “Electronic PHI” means PHI that is transmitted by or maintained in electronic media as defined in the Security Rules.
- G. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
- H. “HITECH” means the privacy and security Breach notification provisions applicable to Business Associate under Title XIII of ARRA.
- I. “Individual” means the person who is the subject of PHI, and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
- J. “Individually Identifiable Health Information” means information that is a subset of health information, including demographic information collected from an individual, and;
 - 1. is created or received by a health care provider, health plan, employer or health care clearinghouse; and
 - 2. relates to the past, present or future physical or mental health 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; and
 - (a) that identifies the individual; or
 - (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- K. “Privacy Rule” means the regulations promulgated under HIPAA by the United States Department of Health and Human Services to protect the privacy of Protected Health Information, including, but not limited to, 45 CFR Part 160 and 45 CFR Part 164, Subpart A and Subpart E.
- L. “Protected Health Information” or “PHI” means Individually Identifiable Health Information transmitted or maintained in any form or medium that (i) is received by Business Associate from Covered Entity, (ii) Business Associate creates for its own purposes from Individually Identifiable Health Information that Business Associate received from Covered Entity, or (iii) is created, received, transmitted or maintained by Business Associate on behalf of Covered Entity. Protected Health Information excludes Individually Identifiable Health Information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. Section 1232(g), records described at 20 U.S.C. Section 1232g(a)(4)(B)(iv), and employment records held by the Covered Entity in its role as employer.
- M. “Security Rule” means the regulations promulgated under HIPAA by the United States Department of Health and Human Services to protect the security of the Electronic Protected Health Information, including, but not limited to, 45 CFR Part 160 and 45 CFR Part 164, Subpart A and Subpart C.

- N. "Unsecured PHI" means PHI that is not secured through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services.
- O. Any terms capitalized, but not otherwise defined, in this Agreement shall have the same meaning as those terms have under HIPAA, the Privacy Rule, the Security Rule and HITECH.

II. Obligations and Activities of Business Associate

A. Prohibited Uses and Disclosures

Business Associate shall not use, access or further disclose PHI other than as permitted or required by this Agreement and as specified in the attached **CONTRACT** or as required by law. Further, Business Associate shall not use PHI in any manner that would constitute a violation of the Privacy Rule or HITECH. Business Associate shall disclose to its employees, subcontractors, agents, or other third parties, and request from Covered Entity, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder.

Business Associate shall not use or disclose PHI for fundraising or marketing purposes. Business Associate shall not disclose PHI to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates; 42 U.S.C. Section 17935(a) and 45 C.F.R. Section 164.522(a)(1)(i)(A). Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of Covered Entity and as permitted by HITECH, 42 U.S.C. Section 17935(d)(2); and 45 C.F.R. Section 164.508 however, this prohibition shall not affect payment by Covered Entity to Business Associate for services provided pursuant to this Agreement.

B. Permitted Uses and Disclosures

1. Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
2. Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation service to Covered Entity as permitted by 45 CFR Section 164.504(e)(2)(i)(B).
3. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR Section 164.502(j)(1).

C. Appropriate Safeguards

Business Associate shall implement the following administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of PHI that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity; and to ensure that any agent or subcontractor to whom Business Associate provides such information agrees to implement reasonable and appropriate safeguards to protect PHI in accordance with the Security Rule under 45 C.F.R., Sections 164.308, 164.310, 164.312, 164.314 and 164.316:

1. Implement policies and procedures to prevent, detect, contain and correct security violations; identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the Business Associate; implement a security awareness and training program for all members of its workforce; implement policies and procedures to prevent those workforce members who should not have access from obtaining access to Covered Entity's Electronic PHI; implement policy and procedures to address security incidents; establish policies and procedures for responding to an emergency or other occurrence that damages systems that contain Electronic PHI; and perform a periodic technical and nontechnical evaluation in response to environmental or operational changes affecting the security of Electronic PHI, including conducting accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity and availability of Electronic PHI, that

establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

2. Implement policies and procedures to limit physical access to Business Associate's electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed; implement policies and procedures that specify the proper functions to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access Electronic PHI; implement physical safeguards for all workstations that access Electronic PHI; restrict access to authorized users; implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain Electronic PHI into and out of a facility and the movement of these items within the facility.
3. Implement technical policies and procedures for electronic information systems that maintain Electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified in 45 C.F.R., Section 164.308 implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use Electronic PHI; implement policies and procedures to protect electronic PHI from improper alteration, destruction, unauthorized access or loss of integrity or availability; including but not limited to, encryption of all workstations, laptops and flash drives that store PHI.
4. Enter into written agreements with agents and subcontractors to whom Business Associate provides Covered Entity's PHI that impose the same restrictions and conditions on such agents and subcontractors that apply to Business Associate with respect to such PHI, and that require compliance with all appropriate safeguards as found in this Agreement.

D. Mitigation

Business Associate shall have procedures in place to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use, access or disclosure of PHI by Business Associate, its agents or subcontractors in violation of the requirements of this Agreement.

E. Reporting of Improper Access, Use or Disclosure or Breach

Business Associate shall report to Covered Entity's Office of Compliance any unauthorized use, access or disclosure of unsecured PHI or any other security incident with respect to PHI no later than one (1) business day upon the discovery of a Breach or suspected Breach consistent with the regulations promulgated under HITECH by the United States Department of Health and Human Services, 45 CFR Part 164, Subpart D. Upon discovery of a Breach or suspected Breach, the Business Associate shall complete the following actions:

1. Provide Covered Entity's Office of Compliance with the following information to include but not limited to:
 - (a) Date the Breach or suspected Breach occurred;
 - (b) Date the Breach or suspected Breach was discovered;
 - (c) Number of staff, employees, subcontractors, agents or other third parties and the titles of each person allegedly involved;
 - (d) Number of potentially affected Patients/Clients; and
 - (e) Description of how the Breach or suspected Breach allegedly occurred.
2. Conduct and document a risk assessment by investigating without reasonable delay and in no case later than five (5) calendar days of discovery of the Breach or suspected Breach to determine the following:
 - (a) The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;
 - (b) The unauthorized person who used PHI or to whom it was made;

- (c) Whether the PHI was actually acquired or viewed; and
 - (d) The extent to which the risk to PHI has been mitigated.
 - 3. Provide a completed risk assessment and investigation documentation to Covered Entity's Office of Compliance within ten (10) calendar days of discovery of the Breach or suspected Breach with decision whether a Breach has occurred.
 - (a) If a Breach has not occurred, notification to Individual(s) is not required.
 - (b) If a Breach has occurred, notification to the Individual(s) is required and Business Associate must provide Covered Entity with affected Individual(s) name and contact information so that Covered Entity can provide notification.
 - 4. Make available to Covered Entity and governing State and Federal agencies in a time and manner designated by Covered Entity or governing State and Federal agencies, any policies, procedures, internal practices and records relating to a Breach or suspected Breach for the purposes of audit or should the Covered Entity reserve the right to conduct its own investigation and analysis.
- F. Access to Protected Health Information
- Business Associate shall provide access to PHI in a Designated Record Set to Covered Entity or to an Individual, at the request or direction of Covered Entity and in the time and manner designated by the Covered Entity. If Business Associate maintains PHI in an electronic format, and an individual requests a copy of such information in electronic form, Business Associate shall provide such information in electronic form as required by of 45 CFR Section 164.524.
- G. Amendment of Protected Health Information
- If Business Associate maintains a Designated Record Set on behalf of the Covered Entity, Business Associate shall make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to, pursuant to 45 CFR Section 164.526, in the time and manner designated by the Covered Entity.
- H. Access to Records
- Business Associate shall make internal practices, books, and records, including policies and procedures and PHI, relating to the use, access and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary of the U.S. Department of Health and Human Services, in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy and Security Rules and patient confidentiality regulations. Anything provided to the Secretary shall also be provided to the Covered Entity upon Covered Entity's request.
- I. Accounting for Disclosures
- Business Associate, its agents and subcontractors shall document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI. Further, Business Associate shall provide to Covered Entity or an Individual, in the time and manner designated by the Covered Entity, information collected in accordance with provision (F.), above, to permit Covered Entity to respond to a request by the Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.
- J. Destruction of Protected Health Information
- Upon termination of this Agreement, Business Associate shall return all PHI required to be retained and return or destroy, with certification of destruction by an officer of Business Associate, all other PHI received from the Covered Entity, or created or received by the Business Associate or its subcontractors, employees or agents on behalf of the Covered Entity. In the event the Business Associate determines that returning the PHI is not feasible, the Business Associate shall provide the Covered Entity with written notification of the conditions that make return not feasible. Business Associate further agrees to extend any and all protections, limitations, and restrictions

contained in this Agreement, to any PHI retained by Business Associate or its subcontractors, employees or agents after the termination of this Agreement, and to limit any further use, access or disclosures to the purposes that make the return or destruction of the PHI infeasible.

K. Breach Pattern or Practice by Covered Entity

Pursuant to 42 U.S.C. Section 17934(b), if the Business Associate knows of a pattern of activity or practice of the Covered Entity that constitutes a material Breach or violation of the Covered Entity's obligations under this Agreement, the Business Associate must take reasonable steps to cure the Breach or end the violation. If the steps are unsuccessful, the Business Associate must terminate the Agreement if feasible, or if termination is not feasible, report the problem to the Secretary of DHHS.

L. Costs Associated to Breach

Business Associate shall be responsible for reasonable costs associated with a Breach. Costs shall be based upon the required notification type as deemed appropriate and necessary by the Covered Entity and shall not be reimbursable under the Agreement at any time. Covered Entity shall determine the method to invoice the Business Associate for said costs. Costs shall incur at the current rates and may include, but are not limited to the following:

1. Postage;
2. Alternative means of notice;
3. Media notification; and
4. Credit monitoring services.

M. Direct Liability

Business Associate may be held directly liable under HIPAA for impermissible uses and disclosures of PHI; failure to provide breach notification to Covered Entity; failure to provide access to a copy of Electronic PHI to covered entity or individual; failure to disclose PHI to the Secretary of the U.S. Department of Health and Human Services when investigating Business Associate's compliance with HIPAA; failure to provide an accounting of disclosures and failure to enter into a business associate agreement with subcontractors.

N. Termination for Cause

Covered Entity may, upon written notice to Business Associate, immediately terminate this agreement, and any related agreements, if Covered Entity determines that Business Associate has breached a material term of this agreement. Covered Entity may, upon written notice to Business Associate, allow Business Associate five (5) business days to cure such breach.

III. Obligations of Covered Entity

- A. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR Section 164.520, to the extent that such limitation may affect Business Associate's use, access or disclosure of PHI.
- B. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an individual to use, access or disclose PHI, to the extent that such changes may affect Business Associate's use, access, maintenance or disclosure of PHI.
- C. Covered Entity shall notify Business Associate of any restriction to the use, access or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR Section 164.522, to the extent that such restriction may affect Business Associate's use, access, maintenance or disclosure of PHI.

IV. General Provisions

A. Remedies

Business Associate agrees that Covered Entity shall be entitled to seek immediate injunctive relief as well as to exercise all other rights and remedies which Covered Entity may have at law or in

equity in the event of an unauthorized use, access or disclosure of PHI by Business Associate or any agent or subcontractor of Business Associate that received PHI from Business Associate.

B. Ownership

The PHI shall be and remain the property of the Covered Entity. Business Associate agrees that it acquires no title or rights to the PHI.

C. Regulatory References

A reference in this Agreement to a section in the Privacy and Security Rules and patient confidentiality regulations means the section as in effect or as amended.

D. 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 and Security Rules and the Health Insurance Portability and Accountability Act and patient confidentiality regulations.

E. Interpretation

Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy and Security Rules and patient confidentiality regulations.

F. Indemnification

Business Associate agrees to indemnify, defend and hold harmless Covered Entity and its authorized officers, employees, agents and volunteers from any and all claims, actions, losses, damages, penalties, injuries, costs and expenses (including costs for reasonable attorney fees) that are caused by or result from the acts or omissions of Business Associate, its officers, employees, agents and subcontractors, with respect to the use, access, maintenance or disclosure of Covered Entity's PHI, including without limitation, any Breach of PHI or any expenses incurred by Covered Entity in providing required Breach notifications.

Addendum A to Business Associates Agreement

These provisions supersede the original Business Associates Agreement (BAA), and is to be considered part of the BAA.

Indemnification

Each of the Parties agrees to be liable for its own conduct in connection with this Business Associate Agreement and to indemnify the other Party against any and all losses therefore. Each of the Parties agrees to indemnify, defend and hold harmless the other Party and its directors, officers, subcontractors, workforce members, affiliates, agents, and representatives from and against any and all third party liabilities, costs, claims, suits, actions, proceedings, demands, losses and liabilities of any kind (including court costs and reasonable attorneys' fees) brought by a third party, arising from or relating to the acts or omissions of that Party or any of its directors, officers, subcontractors, workforce members, affiliates, agents, and representatives in connection with that Party's performance under this Agreement or Service Agreement, without regard to any limitation or exclusion of damages provision otherwise set forth in the Agreement. This Section shall survive the termination of this Agreement.

Access to PHI

Covered Entity acknowledges that all PHI data resides on computer networks and servers controlled by Covered Entity and/or its Agents. Business Associate has very limited access to PHI while providing software support services, and usually only when given access by and supervision from Covered Entity.

Insight mgmt. Systems, Inc. / 2/4/19 / Phylla Manonale

Business Associate/Date & Signature of Officer

Covered Entity/Date & Signature of Officer

Business Associate Addendum for Cloud Services Software as a Service (SaaS)

This Business Associate Addendum for Cloud Services is entered into by and between the County of San Bernardino (County) and Business Associate (Contractor) for the purposes of establishing terms and conditions applicable to the provision of services by Business Associate to the County involving the use of hosted cloud computing services. County and Business Associate agree that the following terms and conditions will apply to the services provided under this addendum and the associated Business Associate Agreement as applicable.

1. DEFINITIONS:

- a) **“Software as a Service (SaaS)”** - The capability provided to the consumer is to use applications made available by the provider running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser or application. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- b) **“Data”** - means any information, formulae, algorithms, or other content that the County, the County's employees, agents and end users upload, create or modify using the SaaS pursuant to this Contract. Data also includes user identification information, Protected Health Information (as defined by the Health Insurance Portability and Accountability Act (HIPAA)) and metadata which may contain Data or from which the Data may be ascertainable.
- c) **“Data Breach”** - means any access, destruction, loss, theft, use, modification or disclosure of Data by an unauthorized party or that is in violation of Contract terms and/or applicable state or federal law.

2. SaaS AVAILABILITY: Unless otherwise stated in the Statement of Work (SOW),

- a) The SaaS shall be available twenty-four (24) hours per day, 365 days per year (excluding agreed-upon maintenance downtime).
- b) If SaaS monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the County shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the SOW.
- c) If SaaS monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the County may terminate the contract for material breach.
- d) Contractor shall provide advance written notice to the County in the manner set forth in the SOW of any major upgrades or changes that will affect the SaaS availability.

3. DATA AVAILABILITY: Unless otherwise stated in the SOW,

- a) The Data shall be available twenty-four (24) hours per day, 365 days per year (excluding agreed-upon maintenance downtime).
- b) If Data monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the County shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the SOW if the County is unable to access the Data as a result of:
 - 1) Acts or omissions of Contractor;
 - 2) Acts or omissions of third parties working on behalf of Contractor;
 - 3) Network compromise, network intrusion, hacks, introduction of viruses, disabling devices, malware and other forms of attack that can disrupt access to Contractor's server, to the extent such attack would have been prevented by Contractor taking reasonable industry standard precautions;
 - 4) Power outages or other telecommunications or Internet failures, to the extent such outages were within Contractor's direct or express control.
- c) If Data monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the County may terminate the contract for material breach.

4. DATA SECURITY:

- a) In addition to the provisions set forth in the Business Associate Agreement, Contractor shall certify to the County:
 - 1) The sufficiency of its security standards, tools, technologies and procedures in providing SaaS under this Contract;
 - 2) Compliance with the following:
 - i. The California Information Practices Act (Civil Code Sections 1798 et seq.);
 - ii. Undergo an annual Statement on Standards for Attestation Engagements (SSAE) 16 Service Organization Control (SOC) 2 Type II audit. Audit results and Contractor's plan to correct any negative findings shall be made available to the County within thirty (30) business days of Contractor's receipt of such results.
- b) Contractor shall implement and maintain all appropriate administrative, physical, technical and procedural safeguards in accordance with section a) above at all times during the term of this Addendum to secure such Data from Data Breach, protect the Data and the SaaS from hacks, introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the County's access to its Data.
- c) Contractor shall allow the County reasonable access to SaaS security logs, latency statistics, and other related SaaS security data that affect this Addendum and the County's Data, at no cost to the County.
- d) Contractor assumes responsibility for the security and confidentiality of the Data under its control.
- e) No Data shall be copied, modified, destroyed or deleted by Contractor other than for normal operation or maintenance of SaaS during the Addendum period without prior written notice to and written approval by the County.
- f) Contractor shall provide access to Data only to those employees, contractors and subcontractors who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor will ensure that, prior to being granted access to Data, staff who perform work under this agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all data protection provisions of this Addendum and the associated Business Associate Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

5. ENCRYPTION: Contractor warrants that all Data will be encrypted in transmission (including via web interface) using Transport Layer Security (TLS) version 1.2 or equivalent and in storage at a level equivalent to or stronger than Advanced Encryption Standard (AES) 128-bit level encryption.

6. DATA LOCATION: All Data will be stored on servers located solely within the Continental United States.

7. RIGHTS TO DATA: The parties agree that as between them, all rights, including all intellectual property rights, in and to Data shall remain the exclusive property of the County, and Contractor has a limited, non-exclusive license to access and use the Data as provided to Contractor solely for performing its obligations under the Contract. Nothing herein shall be construed to confer any license or right to the Data, including user tracking and exception Data within the system, by implication, or otherwise, under copyright or other intellectual property rights, to any third party. Unauthorized use of Data by Contractor or third parties is prohibited. For the purposes of this requirement, the phrase "unauthorized use" means the data mining or processing of data, stored or transmitted by the service, for unrelated commercial purposes, advertising or advertising-related purposes, or for any other purpose other than security or service delivery analysis that is not explicitly authorized.

8. TRANSITION PERIOD:

- a) For ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Contractor shall assist the County in extracting and/or transitioning all Data in the format determined by the County ("Transition Period").
- b) The Transition Period may be modified in the SOW or as agreed upon in writing by the parties in a contract amendment.
- c) During the Transition Period, SaaS and Data access shall continue to be made available to the County without alteration.

- d) Contractor agrees to compensate the County for damages or losses the County incurs as a result of Contractor's failure to comply with this section.
- e) Unless otherwise stated in the SOW, the Contractor shall permanently destroy or render inaccessible any portion of the Data in Contractor's and/or subcontractor's possession or control following the expiration of all obligations in this section. Within thirty (30) days, Contractor shall issue a written statement to the County confirming the destruction or inaccessibility of the County's Data.
- f) The County at its option, may purchase additional transition services as agreed upon in the SOW.

9. DISASTER RECOVERY/BUSINESS CONTINUITY: Unless otherwise stated in the Statement of Work,

- a) In the event of disaster or catastrophic failure that results in significant Data loss or extended loss of access to Data, Contractor shall notify the County by the fastest means available and also in writing. Contractor shall provide such notification within twenty-four (24) hours after Contractor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Contractor shall inform the County of:
 - 1) The scale and quantity of the Data loss;
 - 2) What Contractor has done or will do to recover the Data and mitigate any deleterious effect of the Data loss; and
 - 3) What corrective action Contractor has taken or will take to prevent future Data loss.
- b) If Contractor fails to respond immediately and remedy the failure, the County may exercise its options for assessing damages or other remedies.
- c) Contractor shall restore continuity of SaaS, restore Data, restore accessibility of Data, and repair SaaS as needed to meet the Data and SaaS Availability requirements under this Addendum. Failure to do so may result in the County exercising its options for assessing damages or other remedies.
- d) Contractor shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with the County. The County and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Contractor shall cooperate fully with the County, its agents and law enforcement.

10. EXAMINATION AND AUDIT: Unless otherwise stated in the Statement of Work:

- a) Upon advance written request, Contractor agrees that the County or its designated representative shall have access to Contractor's SaaS operational documentation and records, including online inspections that relate to the security of the SaaS product purchased by the County.
- b) Contractor shall allow the County, its authorized agents, or a mutually acceptable third party to test that controls are in place and working as intended. Tests may include, but not be limited to, the following:
 - 1) Operating system/network vulnerability scans,
 - 2) Web application vulnerability scans,
 - 3) Database application vulnerability scans, and
 - 4) Any other scans to be performed by the County or representatives on behalf of the County.
- c) After any significant Data loss or Data Breach or as a result of any disaster or catastrophic failure, Contractor will at its expense have an independent, industry-recognized, County-approved third party perform an information security audit. The audit results shall be shared with the County within seven (7) days of Contractor's receipt of such results. Upon Contractor receiving the results of the audit, Contractor will provide the County with written evidence of planned remediation within thirty (30) days and promptly modify its security measures in order to meet its obligations under this Contract.

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

12. INSURANCE REQUIREMENTS: Contractor shall, at its own expense, secure and maintain for the term of this contract, Cyber Liability Insurance with limits of no less than \$1,000,000 for each occurrence or event with an annual aggregate of \$2,000,000 covering claims involving privacy violations, information theft, damage to or destruction of electronic information, intentional and/or unintentional release of private information, alteration of electronic information, extortion and network security. The policy shall cover breach response cost as well as any regulatory fines and penalties.

13. DATA SEPARATION: Data must be partitioned from other data in such a manner that access to it will not be impacted or forfeited due to e-discovery, search and seizure or other actions by third parties obtaining or attempting to obtain Service Provider's records, information or data for reasons or activities that are not directly related to Customer's business.

[END OF DOCUMENT]



Insight

Management Systems, Inc.

ATTACHMENT D
17337 Ventura Blvd. Suite 307

Encino CA 91316

December 3, 2020

County of San Bernardino
Family Health Radiology Department
606 E. Mill Street
San Bernardino, CA 92415

**1. Re: OmniCare Breast, Lung and/or Disease Management System
Annual License, Maintenance and HIPAA BAA Renewal**

| | |
|------------------------------------|--------------------------|
| Current License Expiration: | <u>02/28/2021</u> |
|------------------------------------|--------------------------|

**** Send in this Renewal Form by the Discount Date to save an extra 6% ****

Dear Stewart,

Thank you for your continued support. We value you as a client and the relationship that we have built. This is a partnership, and as your needs change, OmniCare is growing and changing as well. There are many resources available to help you get the most out of your OmniCare system, so please don't hesitate to contact our customer support department.

Please take this time to review this information and return your signed order form, along with payment and/or a purchase order.

Cordially,

Shella Manansala
(818) 385-0123 x108 sm@insightmed.com

2. What's new for this upcoming renewal year:

- Version 7.6.9, and all the new features that come with it
- Integrated Tyrer Cuzick V8 Risk Assessment and High Risk Patient Management
- LCSR 2.0, AJCC V8
- Incidental Findings Patient Management
- Improved Navigation and Survivorship Care Plans
- Enhanced integration with EHR
- Breast and Lung imaging workflow improvements



OmniCare: Annual License, Maintenance and HIPAA BAA Renewal Invoice

| | | |
|---|----------------------------|--------------------------------|
| Client: County of San Bernardino Family Health Radiology Department 606 E. Mill Street San Bernardino, CA 92415 | License Expiration: | 02/28/2021 |
| | Primary Contact: | Ivan Pinto; Lori Geist |
| | OmniCare System | Version 7.6.5 |
| | Client Since: | August 2013 **8 Years** |
| Insight Contact: Shella Manansala: sm@insightmed.com , 800-643-0123 x108 | | |

Renewal of your contract is required to continue OmniCare and will extend our HIPAA Business Associates Agreement for another year.
 All other terms of Insight's Standard Licensing Agreement apply

- 3. OmniCare Annual Software License Renewal (required) through: 02/28/2022**
4. HIPAA Business Associates Agreement Renewal
5. Annual Maintenance and Support: includes
 - a. OmniCare software updates
 - b. Unlimited support and training: phone, email, and on-line
 - c. Continued software compliance with MQSA, ACR BiRads, NMD and LCSR
6. Software Updates as they become available: Next Release will be Version 7.6.9
7. Annual Software Review & Analysis (contact us to schedule)

| | |
|--|-------------------|
| Total Due: | \$2,999.00 |
| 6% discount if returned before: 01/31/2021: | |
| Highly Recommended Options: Order with annual renewal and enjoy big savings | |
| Total Renewal and Options Amount: | |

Please complete this section and email to sm@insightmed.com or fax to 818-385-0124

Approved By: _____ **Title:** _____

Signature: _____ **Phone / email:** _____

Check one:

____ Purchase Order: #: _____ Check Enclosed: #: _____

____ Credit Card: #: _____ (visa, mc, amex) Exp Date: _____ SecCode: _____

discounts will be reduced by 3% for credit card payments

Insight Management Systems, Inc.
Software and Services - Standard License Agreement

By purchasing, renting, installing, and/or using the software and services provided by Insight Management Systems, Inc. ("Insight", "Licensor"), you, the purchaser or user(s) ("Licensee", "you"), hereby agrees to be bound to the terms contained in this Software and Services License Agreement ("Agreement").

| | |
|--|--|
| <p><u>"Insight"</u> Insight Management Systems, Inc. 17337 Ventura Boulevard, Suite 307 Encino, CA 91316 818-385-0123</p> | <p><u>"Client"</u> County of San Bernardino 606 E. Mill Street San Bernardino, CA 92415 (888)818-8988</p> |
|--|--|

Software and Services

Insight has provided you, or will provide you, with the software and services described in the accompanying purchase proposal. The purchase proposal sets forth the features, options, services and prices of the software and services to be provided by Insight. The software program has been provided, or will be provided, on standard media; CD, Diskette, or electronically for installation onto clients compatible hardware systems by either Insight or your staff, as provided by the proposal. Any "Services" listed in the proposal will also be provided by Insight with the cooperation of your staff and information systems personnel.

Licensure

Insight develops, markets and supports computer software applications and related services for the healthcare environment, including, but not limited to, Insight's OmniCare Family of Healthcare Information Systems, and the system you, the Licensee, desires to license (hereinafter referred to as "Software"). THEREFORE, upon your acceptance of the terms of this Agreement and in exchange for your payment of the fees specified in your proposal, Insight grants you a non-exclusive, nontransferable license to install and render the Software operational on the terms set forth herein. In order to maintain Licensure and the rights to use Software, Licensee must renew an Annual License and Support Agreement and pay fees specified in your proposal.

This software product is licensed by Insight to the original purchaser and for use only on approved computer hardware systems. "Software" configurations will remain the same unless altered in written form by Insight.

Exact software license and feature configuration is outlined in your proposal. If this is a single user version, then it may be assigned to an individual computer. If this is a multi user version, then you may use this on a single file server, with the specified number of users. This license is only valid for management of one physical facility unless otherwise stated in writing by Insight.

License Restrictions:

The license provided for in this Agreement extends to your use of the features and modules that you are licensing as listed on your proposal and original invoice. You may copy the Software and data onto other media for backup purposes only.

You may not distribute this Software or underlying code, data, and/or trade secrets in any form to any other parties or any computers not specifically listed in the proposal or activate or use any features or modules that are not part of your software purchase.

Ownership Interests:

Licensor owns and retains all right, title, and interest in the Software and related documentation and materials. This Agreement does not transfer ownership rights to the Licensee or any third party. Other than as stated above, you may not use, copy, modify, or create derivative works based on the Software. In addition, you may not transfer the program or any copy, modification or portion, in whole or part, except as expressly provided for in this license. You may not remove any copyright and trademark notices on the Software and related documentation, including the startup messages contained in the programs and shall take other necessary steps to protect Licensor's intellectual property rights. You may not transfer possession of any copy, modification or merged portion of the program to another party.

Warranties, Disclaimers, Limitations:

Insight warrants to you that it is the owner of the copyright to the product listed above, and will indemnify you against all claims from third parties challenging such ownership, provided that you provide prompt notice of any such claim and permit Insight to defend or settle the claim. Before making copies of this program you will ascertain its fitness for your use, and check that it is sufficiently free from error or malfunction for use by the intended recipients.

The programs are warranted by Insight to conform substantially to the program's documentation and Insight's published specifications, provided that they are used as set forth herein and in the documentation. The physical diskettes/CD and documentation enclosed in this package are warranted by Insight to be free from defects in materials and workmanship that prevent you from operating the programs. This warranty does not cover defects caused by the Licensee's misuse of the Software subsequent to delivery.

Insight will replace defective diskettes, CD or documentation, or correct substantial program errors free of charge during the software support period. The support service period is referred to in the proposal and may be extended annually for a fee. These are your sole remedies for any breach of warranty.

Except as otherwise provided for in this Agreement, the programs are licensed and the documentation and other files on the diskettes are provided "AS IS", without any warranty as to performance, accuracy, or freedom from error, or as to any results generated through use of such material, including, without limitation, any implied warranties of merchantability or fitness for a particular purpose. There is no warranty that the Software is compatible with all equipment and software configurations. You assume the entire risk as to the result and performance of this product. Insight specifically does not warrant that the program will meet your changing requirements or operate without interruption or error.

Insight's obligation to replace defective media, documentation and programs, as provided above, shall be your sole and exclusive remedy for any and all claims against Insight arising out of, or in connection with, this product, whether made or suffered by you or any other person and whether based in contract or in tort. Under no circumstances shall Insight be liable for indirect, consequential, special or exemplary damages, whether based in contract or tort, including, but not limited to, loss of revenue, data or profits, and lost business or other economic loss arising out of, or in connection with, this product or your use of or inability to use the diskettes/CD, the documentation or the program(s). Licensor's liability for damages under this Agreement, whether based in contract or in tort, shall not exceed one million dollars (US\$1,000,000). This limitation shall not apply to claims arising under Licensor's indemnity obligations or from Licensor's gross negligence, willful misconduct or violations of law.

In some instances Insight may provide services to you related to your License including, but not limited to, data conversions, interfaces, technical support, information on regulatory compliance, and report / letter / & screen customization. While Insight takes measures to insure the accuracy and quality of the services it provides, in no way does Insight make any warranties, express or implied, oral or written, with respect to such work and Licensor agrees to hold it blameless for any and all damages that result therefrom.

Installation, "Acceptance" and Acceptance Testing

Time for Testing: Licensee shall have forty five (45) days from the installation date as the Testing Period to test the components of the System for each System Installation. These components are defined in the "Confidential Systems Proposal".

Written notice of Defect: If, for a particular Installation, the Licensed Materials and/or specific component does not perform in accordance with the Documentation, and does not involve other vendors of Licensee, then Licensee shall submit to Licensor a Written Notice of Defect, specifying the component and specific failure of performance. If after 30 days of testing, no notice of defects have been sent in writing by Licensee to Licensor, Acceptance is implicitly granted.

Corrections: Licensor will correct, modify, or improve the items declared in the Written Notice of Defect within 60 days, or a time mutually agreed upon, of receipt, and will notify Licensee that the Licensed Materials are again ready to be verified for that particular Installation. Licensee will then have the greater of fourteen (14) calendar days or the remainder of the Testing Period, or a time mutually agreed upon in writing by both parties to retest the declared items to determine whether Licensor has cured the Defects listed in the Written Notice of Defects. If Licensee determines that the System still does not perform in accordance with the Documentation, Licensee shall issue another Written Notice of Defects or otherwise inform Licensor of such remaining Defects. Failure of Licensee to notify Licensor of Defects during said fourteen (14) calendar day re-testing period shall constitute Licensee's acceptance of the System. This process will be repeated as may be necessary until Licensee provides an Acceptance Certificate to Licensor provided, however, that the total period of time that may be spent in the procedure described in this paragraph shall not exceed 120 days from the beginning of

the Installation Period, or a time mutually agreed upon in writing by both parties, after which time Licensee shall no longer be obligated to accept such corrections from Licensor and such failure by Licensor to cure the Defects of the System shall be deemed a material breach of this Agreement and subject to termination of agreement, unless Licensor's failure to cure is substantially attributable to Licensee and/or other vendors of Licensee.

Acceptance: For each Installation, during the Testing Period, Licensee determines that the System does perform in accordance with the Documentation or if Licensor cures all Defects in any and all Written Notice of Defects, Licensee will present to Licensor an Acceptance Certificate that Licensee accepts the System for shall not rescind or modify prior acceptance for a specific Installation.

Termination:

Upon your failure to comply with any or all of the terms and conditions of this Agreement, your license(s) to use this product will terminate immediately. Failure to renew and pay for your Annual License and Support Agreement will result in termination. In addition, Licensor may terminate this Agreement if there is a change in control of the Licensee, whether by sale of assets, stock or otherwise, or if Licensee initiates a proceeding for protection under the bankruptcy laws of the United States or similar laws. Upon written notice by Insight of your license violation and subsequent termination, you must immediately cease to use the software product(s), return all copies of the software and supporting literature, and remove the Software from all installed systems. Only the data files may remain in your possession.

This license agreement may not be assigned by you to others without the written consent of Insight. Costs for authorized transfers will be determined by Insight. This license agreement shall be binding upon the respective successors and assigns of the parties.

Confidentiality:

Licensee acknowledges that the Software and related documentation, and all information relating to the business and operations of the Licensor that Licensee learns or has learned during or prior to the term of this Agreement, may be the valuable, confidential and proprietary information of the Licensor. During the period this Agreement is in effect, and at all times afterwards, Licensee and its employees, contractors, consultants and agents will safeguard the confidential information with the same degree of care that it uses to protect its own confidential information, maintain the confidentiality of this information, not use the information except as permitted under this Agreement, and not disseminate, disclose, sell, publish, or otherwise make available the information to any third party without the prior written consent of Licensor, unless otherwise required by applicable law.

During the course of providing support services, Insight staff will have access to some patient information. Insight agrees to uphold complete patient confidentiality and non-disclosure of any and all Client patient information to any third party and use this information solely for support purposes.

Software Updates:

On occasion, Insight develops and releases software updates that add or enhance features that may assist Client in their compliance with existing, new or modified regulatory issues. These software updates may be made available to all Clients on current versions and License and Support contracts or those who have purchased the updates. It is the Client's sole responsibility to ensure that all updates are installed and their working version of the Insight software is the current release.

General Regulatory Compliance:

Nothing in this Agreement shall be construed as creating any obligation on the part of Insight to assure Licensee's compliance with any and/or all federal, state and local laws or other regulatory bodies which are applicable to Licensee, including, but not limited to HIPAA or MQSA. The Parties acknowledge and agree that Insight makes no representation, promise or warranty that Client's licensure and/or use of Insight's Software or services will result in Licensee's compliance with any and/or all regulations and requirements. Moreover, Licensee acknowledges that nothing in this Agreement shall be construed as obligating Insight to provide any service and/or product which is intended to, or does, ensure Licensee's compliance with any and/or all regulations and/or requirements.

HIPAA Business Associates Addendum is a separate agreement and not part of This Standard License Agreement.

Export Controls:

The Software, documentation and all underlying information or technology may not be exported or re-exported into any country to which the U.S. has embargoed goods, or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. Licensee shall not export the Software or Documentation or any underlying information or technology to any facility in violation of these or other applicable laws

and regulations. Licensee represents and warrants that it is not a national or resident of, or located in or under the control of, any country subject to such export controls.

Waiver:

This Agreement may not be modified or amended except in a writing signed by an authorized officer of each party. The failure of either party to enforce any provision of the Agreement shall not be deemed a waiver of the provisions or of the right of such party thereafter to enforce that or any other provision.

Independent Contractor:

Nothing in this Agreement shall be deemed to create an employer/employee, principal/agent, or joint venture relationship. Neither party shall have the authority to enter into any contracts on behalf of the other party.

Governing Law and Jurisdiction:

This Agreement shall be governed by and construed in accordance with the laws of the State of California. The parties consent to personal jurisdiction in California for any proceeding initiated relative to this Agreement.

Severability:

In case any provision of this Agreement is held to be invalid, unenforceable, or illegal, any such provision will be severed from this Agreement, and such invalidity, unenforceability, or illegality will not affect any other provisions of this Agreement.

[END OF DOCUMENT]