FIVOS, Inc.
BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement"), effective as of May 1, 2026. ("Effective Date"), is made by and between San Bernardino County on behalf of **Arrowhead Regional Medical Center** on behalf of itself and its Affiliates (collectively, "Covered Entity"), having a facility at 400 N. Pepper Ave, Colton, CA 92324 and **Fivos, Inc.** on behalf of itself and all of its Affiliates ("Business Associate"), having a principal place of business at 8 Commerce Avenue, West Lebanon, NH 03784.

WHEREAS, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health Act ("**HITECH**") adopted as part of the American Recovery and Reinvestment Act of 2009, HIPAA Omnibus Final Rule modifications of 2013, and regulations promulgated thereunder, may require certain entities to place certain provisions in their agreements with third parties who use/disclose certain patient information;

WHEREAS. Covered Entity and Business Associate are parties to that certain Underlying Agreement (as defined below), pursuant to which Covered Entity will provide Protected Health Information (as defined below) to Business Associate;

WHEREAS, the parties have determined that it is in their respective interests to comply with HIPAA and related regulations and now desire to agree to terms and conditions concerning the use and disclosure of such Protected Health Information; and

NOW, THEREFORE, in consideration of the foregoing premises and mutual covenants and promises contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1.0 Definitions.

1.1 "Administrative safeguards" shall mean administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information as described in 45 C.F.R. 164.304.

1.2 "Affiliate" refers to, in relation to a party, any entity, which directly or indirectly controls, is controlled by, or is under common control with, such party.

1.3 "Breach" shall have the same meaning given to such term under the HIPAA Regulations [45 C.F.R. §164.402] and the HITECH Act [42 U.S.C. §§17921 et seq.], and includes the definition set forth in 22 California Code of Regulations (C.C.R.) § 79901(b).

1.4 Business Associate shall have the same meaning given to such term under the Privacy Rule, the Security Rule, and the HITECH Act, including but not limited to 42 U.S.C. §17921 and 45 C.F.R. §160.103, and includes the definition set forth in 22 C.C.R. § 79901(c).

1.5 Covered Entity shall have the same meaning given to such term as under the Privacy Rule and Security Rule, including, but not limited to 45 C.F.R. §160.103.

1.6 "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 C.F.R. 164.501.

1.7 "Disclosure" shall mean the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information as described in 45 C.F.R. 160.103.

1.8 "Electronic Protected Health Information" or "EPHI" means PHI that is maintained in or transmitted by electronic media as defined in the Security Rule at 45 C.F.R. 160.103.

1.9 "Individual" shall have the same meaning as the term "individual" in 45 C.F.R. 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. 164.502(g).

1.10 Medical Information shall have the same meaning given to such term under 22 C.C.R. §79901(i)

1.11 "Physical safeguards" shall mean physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion as described in 45 C.F.R. 164.304.

1.12 "Privacy Rule" means the regulations promulgated under HIPAA by the United States Department of Health and Human Services (HHS) to protect the privacy of Protected Health Information, including, but not limited to, 45 C.F.R. part 160 and part 164, subparts A and E.

1.13 "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 C.F.R. 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity and includes Medical Information.

1.14 "Reasonable cause" shall mean an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect as described in 45 C.F.R. 160.401.

1.15 "Required By Law" shall have the same meaning as the term "required by law" in 45 C.F.R. 164.103.

1.16 "Secretary" shall mean the Secretary of the United States Department of Health and Human Service ("HHS") or his/her designee.

1.17 "Security Rule" shall mean the regulations promulgated under HIPAA by HHS to protect the security of ePHI, including, but not limited to, 45 C.F.R. parts 160, 162, and 164, subparts A and C.

1.18 "Subcontractor" shall mean a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate as described in 45 C.F.R. 160.103.

1.19 "Underlying Agreement" shall mean the arrangement(s) or written agreement(s) between Covered Entity and Business Associate that involve(s) the use or disclosure of Protected Health Information.

1.20 “Unsecured PHI” shall have the same meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act, including, but not limited to 42 U.S.C. §17932, subdivision (h)..

1.1 "Unsuccessful Security Incident" shall means, without limitation, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful logon attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of Protected Health Information.

1.2 “Workforce” shall mean employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate as described in 45 C.F.R. 160.103.

2.0 <u>Obligations and Activities of Business Associate</u>.

2.1 Business Associate agrees to use appropriate Administrative safeguards and Physical safeguards to ensure the confidentiality, integrity, and availability of all electronic Protected Health Information provided by Covered Entity or created, received, maintained, or transmitted by Business Associate pursuant to the Underlying Agreement, as required by 45 C.F.R. 164.306.

2.2 Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required by Law.

2.3 Business Associate agrees to use appropriate Administrative safeguards and Physical safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

2.4 Business Associate agrees to use reasonable efforts to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

2.5 Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware. Upon discovery of a Breach or suspected Breach, Business Associate shall complete the following actions:

2.5.1 Provide Covered Entity’s Office of Compliance with the following information to include but not limited to:

2.5.1.1 Name and address of the facility where the Breach occurred;

2.5.1.2 Date and time the Breach or suspected Breach occurred;

2.5.1.3 Date and time the Breach or suspected Breach was discovered or Detected;

2.5.1.4 Number of staff, employees, subcontractors, agents or other third parties and the names and titles of each person allegedly involved, including the person who performed the Breach, witnessed the Breach, used the PHI, or the person to whom the disclosure was made;

2.5.1.5 Name of patient(s) affected;

2.5.1.6 Number of potentially affected Individual(s) with contact information;

2.5.1.7 Description of how the Breach or suspected Breach allegedly occurred; and

2.5.1.8 Description of the PHI that was Breached, including the nature and extent of the PHI involved, including the types of individually identifiable information and the likelihood of re-identification.

2.5.2 Conduct and document a risk assessment by investigating without unreasonable delay and in no case later than five (5) business days of discovery of the Breach or suspected Breach to determine the following:

2.5.2.1 The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;

2.5.2.2 The unauthorized person who had access to the PHI;

2.5.2.3 Whether the PHI was actually acquired or viewed; and

2.5.2.4 The extent to which the risk to PHI has been mitigated.

2.5.3 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 a determination as to whether a Breach has occurred. At the discretion of Covered Entity, additional information may be requested.

2.5.3.1 If Business Associate and Covered Entity agree that a Breach has not occurred, notification to Individual(s) is not required.

2.5.3.2 If a Breach has occurred, notification to the Individual(s) is required and Business Associate must provide Covered Entity with affected Individual(s) name so that Covered Entity can provide notification.

2.5.3.3 The risk assessment and investigation documentation provided by Business Associate to Covered Entity shall, at a minimum, include a description of any corrective or mitigation actions taken by Business Associate.

2.5.4 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.

2.6 Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees in writing to functionally the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

2.7 If Business Associate maintains Protected Health Information in a Designated Record Set, Business Associate agrees to provide access, within ten (10) business days of Covered Entity's request, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. 164.524.

2.8 If Business Associate maintains Protected Health Information in a Designated Record Set, Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. 164.526 at the request of Covered Entity within ten (10) business days of such request.

2.9 Business Associate agrees to make internal practices, books, and records relating to the use, access, and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance

with the Privacy Rule and Security Rule and patient confidentiality regulations. Any documentation provided to the Secretary shall also be provided to the Covered Entity upon request.

2.10 Business Associate agrees to document such disclosures of Protected Health Information 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 Protected Health Information in accordance with 45 C.F.R. 164.528.

2.11 Business Associate agrees to provide to Covered Entity or an Individual, within ten (10) business days of request, information collected in accordance with Section 2.10 of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. 164.528.

2.12 Business Associate shall 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.

2.13 Security Rule Provisions. If Business Associate creates, receives, maintains, or transmits EPHI on Covered Entity's behalf, Business Associate shall:

2.13.1 implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity, in accordance with 45 C.F.R. sections 164.308, 164.310, 164.312 and 164.316. [45 C.F.R. sections 164.504(e)(2)(ii)(b) and 164.308(b).];

2.13.2 ensure that any Subcontractor that creates, receives, maintains, or transmits electronic Protected Health Information on behalf of Business Associate in connection with the Underlying Agreement agrees to comply with the applicable HIPAA requirements and agrees to implement reasonable and appropriate Administrative safeguards and Physical safeguards to protect such EPHI; and

2.13.3 without unreasonable delay following the completion of internal investigations for known or suspected Security Incidents, report to Covered Entity any Security Incident of which it becomes aware; provided, however, that the parties acknowledge and agree that this section constitutes notice by Business Associate to Covered Entity of the ongoing existence of, occurrence of, and attempts by third parties that constitute Unsuccessful Security Incidents for which no additional notice to Covered Entity shall be required.

2.13.4 provide notice of a Breach of Unsecured Protected Health Information to Covered Entity without unreasonable delay and in no case later than ten (10) business days following the discovery of a Breach in accordance with 45 C.F.R. § 164.410. A Breach shall be treated as 'discovered' by Business Associate as of the first day on which such Breach is known to Business Associate or by exercising reasonable diligence, would have been known to Business Associate. Business Associate's notification of Breach to Covered Entity shall be made in writing, and shall include, to the extent practicable, the identification of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during the Breach.

2.13.5 Within ninety (90) days of termination of this Agreement, Business Associate shall destroy or return Covered Entity's PHI to the extent feasible.

2.13.6 In accordance with 45 C.F.R. §164.316, Business Associate shall maintain reasonable and appropriate written policies and procedures for its privacy and security program in order to comply with the standards, implementation specifications, or any other requirements of the Privacy Rule and applicable provisions of the Security Rule. =

2.13.7 Business Associate shall provide appropriate training for its workforce on the requirements of the Privacy Rule and Security Rule as those regulations affect the proper handling, use confidentiality and disclosure of the Covered Entity's PHI. Such training will include specific guidance relating to sanctions against workforce members who fail to comply with privacy and security policies and procedures and the obligations of the Business Associate under this Agreement.

3.0 <u>Permitted Uses and Disclosures by Business Associate</u>.

3.1 <u>General Use and Disclosure Provisions</u>.

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in Underlying Agreement.

3.2 <u>Specific Use and Disclosure Provisions</u>.

3.2.1 Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information (i) for the proper management and administration of the Business Associate; (ii) to carry out the legal responsibilities of the Business Associate. Prior to making any other disclosures, Business Associate must obtain a written authorization from the Individual.

3.2.2 Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration or to carry out the legal responsibilities of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable written assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and a written agreement from the person to immediately notify the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached. [42 U.S.C. §17932; 45 C.F.R. §§164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)]

3.2.3 Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. 164.504(e)(2)(i)(B).

3.2.4 Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. 164.502(j)(1).

3.2.5 Business Associate may de-identify any and all Protected Health Information created or received by Business Associate under this Agreement; provided, however, that the de-identification conforms to the requirements of the Privacy Rule. Such resulting de-identified information would not be subject to the terms of this Agreement and may be used or disclosed by Business Associate for quality improvement or other commercial purposes without compensation to Covered Entity.

3.2.6 Business Associate may partially de-identify any PHI to create a Limited Data Set, provided such partial de-identification conforms to the Limited Data Set requirements of 45 CFR 164.514(e)(2).

4.0 Prohibited Uses and Disclosures

4.1 Business Associate shall not use, access or further disclose PHI other than as permitted or required by this Agreement 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 the HITECH Act. 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.

4.2 Business Associate shall not use or disclose PHI for fundraising or marketing purposes.

4.3 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 the HITECH Act (42 U.S.C. §17935(d)(2); and 45 C.F.R. §164.508); however, this prohibition shall not affect payment by Covered Entity to Business Associate for services provided pursuant to this Agreement.

5.0 Obligations of Covered Entity.

5.1 Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions.

5.1.1 Covered Entity agrees to provide Business Associate with the minimum necessary amount of Protected Health Information required to perform the services set forth in the Underlying Agreement.

5.1.2 Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 C.F.R. 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

5.1.3 Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use, access, or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

5.1.4 Covered Entity shall notify Business Associate of any restriction to the use, access, or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

5.1.5 Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's notice of privacy practices in accordance with 45 C.F.R. §164.520 to the extent that such may affect Business Associate's use, access, maintenance or disclosure of PHI.

5.1.6 Covered Entity shall obtain any consent, authorization or permission that may be required by the Privacy Rule or applicable state laws and/or regulations prior to furnishing Business Associate the Protected Health Information pertaining to an individual.

5.1.7 Covered Entity will inform Business Associate of any specific state laws that it believes are applicable to Protected Health Information submitted by Covered Entity and would require Business Associate to take compliance steps beyond those required under HIPAA.

5.2 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 the Privacy Rule if done by Covered Entity.

6.0 Term and Termination.

6.1 Term. The Term of this Agreement shall be effective as of the Effective 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. If it is infeasible to return or destroy Protected Health Information, protections of this Agreement shall extend to such information, in accordance with the termination provisions in this Section 6.5.2.

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

6.2.1 Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement and the Underlying Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

6.2.2 Immediately terminate this Agreement and the Underlying Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

6.2.2.1 If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

6.3 Termination Without Cause. Either party may terminate this Agreement with at least thirty (30) days written notice to the other party.

6.4 Notwithstanding anything in the foregoing, this Agreement may not be terminated by either party if the Underlying Agreement is in effect and federal law requires this Agreement for the provision of the services by Business Associate under the Underlying Agreement.

6.5 Effect of Termination.

6.5.1 Except as provided in Section 6.5.2, upon termination 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. Business Associate must follow established policies and procedures to ensure PHI is safeguarded and disposed of adequately in accordance with 45 C.F.R. §164.310, and must submit to the Covered Entity a certification of destruction of PHI. For destruction of EPHI, the National Institute of Standards and Technology (NIST) guidelines must be followed.

6.5.2 In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity written notification of the conditions that make return or destruction infeasible. Upon Covered Entity's receipt of Business Associate's written notification 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.

7.0 Direct Liability

Business Associate may be held directly liable under HIPAA and California law for impermissible uses and disclosures of PHI; failure to provide breach notification to Covered Entity; failure to provide access to a copy of PHI or ePHI to Covered Entity or individual; failure to disclose PHI to the Secretary of HHS 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.

8.0 Indemnification and Limitation of Liability

8.1 Both parties agrees to indemnify, defend and hold harmless the other party 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 the indemnifying aprty, 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 under federal and state laws.

8.2 **Limitation of Liability. BUSINESS ASSOCIATE'S LIABILITY TO COVERED ENTITY FOR ANY LOSSES OR INDIRECT DAMAGES, IN CONTRACT, TORT OR OTHERWISE, ARISING OUT OF THE SUBJECT MATTER OF THIS AGREEMENT SHALL BE LIMITED TO THOSE ACTUAL AND DIRECT DAMAGES WHICH ARE REASONABLY INCURRED BY COVERED ENTITY AND SHALL NOT EXCEED ONE MILLION DOLLARS ($1,000,000). BUSINESS ASSOCIATE SHALL NOT BE LIABLE TO COVERED ENTITY FOR ANY SPECIAL, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES ARISING FROM OR AS A RESULT OF ANY DELAY, OMISSIONS, OR ERROR IN THE ELECTRONIC TRANSMISSION OR RECEIPT OF ANY INFORMATION PURSUANT TO THIS AGREEMENT, EVEN IF COVERED ENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**

9.0 Judicial or Administrative Proceedings

Covered Entity may terminate the Contract, effective immediately, if (i) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws or (ii) a finding or stipulation is made in any administrative or civil proceeding in which the Business Associate has been joined that the Business Associate has violated any standard or requirement of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws.

10.0 Assistance in Litigation or Administrative Proceedings

Business Associate shall make itself, and any employees, or agents assisting Business Associate in the performance of its obligations under the Agreement, available to Covered Entity, at no cost to Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity, its directors, officers, or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where Business Associate or its subcontractor, employee or agent is a named adverse party. Business Associate shall use commercially reasonable efforts to also cause its Subcontractor's and agents, assisting Business Associate in the performance of its obligations under the Agreement, to cooperate with the Covered Entity to facilitate resolving any allegations and the settlement or defense of the Covered Entity.

11.0 Miscellaneous.

11.1 Intentionally omitted..

11.2 Regulatory References. A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.

11.3 Amendment. The parties acknowledge that state and federal laws related to privacy and security of PHI are rapidly evolving and that amendment of the Contract or this Agreement may be required to ensure compliance with such developments. The parties agree to negotiate in good faith to amend this Agreement from time to time as is necessary for either party or both parties to comply with applicable law. If either party does not agree to so amend this Agreement within 30 days after receiving a request for amendment from the other, either party may terminate the Agreement upon written notice. To the extent an amendment to this Agreement is required by law and this Agreement has not been so amended to comply with the applicable law in a timely manner, the amendment required by law shall be deemed to be incorporated into this Agreement automatically and without further action required by either of the parties. Subject to the foregoing, this Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed and agreed to by Business Associate and Covered Entity.

11.4 Assignment. Neither party will assign this Agreement or any part thereof to any third party without prior written consent to the other party (which shall not be unreasonably withheld) provided.

11.5 Survival. The respective rights and obligations of Covered Entity and Business Associate relating to protecting the confidentiality or a patient's PHI shall survive the termination of the Underlying Agreement or this Agreement.

11.6 Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule and Security Rule, the HITECH Act, and all applicable patient confidentiality regulations.

11.7 Construction of Terms. The terms of this Agreement shall be construed in light of any applicable interpretation or guidance on HIPAA, the Privacy Rule, and/or the Security Rule issued by HHS or the Office of Civil Rights ("OCR") from time to time.

11.8 No Third Party Beneficiaries. Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

11.9 Contradictory Terms. Any provision of the Underlying Agreement that is directly contradictory to one or more terms of this Agreement ("Contradictory Term") shall be superseded by the terms of this Agreement as of the Effective Date of this Agreement to the extent and only to the extent of the contradiction, only for the purpose of the Covered Entity's compliance with the Privacy Rule and Security Rule and only to the extent that it is reasonably impossible to comply with both the Contradictory Term and the terms of this Agreement.

11.10 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.

11.11 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.

11.12 Compliance with State Law. In addition to HIPAA and all applicable HIPAA Regulations, Business Associate acknowledges that Business Associate and Covered Entity may have confidentiality, privacy, and breach notification obligations under State law, including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code §56, et seq. ("CMIA")), and 22 C.C.R. § 79001 et seq. If any provisions of this Agreement or HIPAA Regulations or the HITECH Act conflict with CMIA or any other California State law regarding the degree of protection provided for PHI and patient medical records, then Business Associate shall comply with the more restrictive requirements.

11.13 Dispute Resolution. Covered Entity and Business Associate agree they will establish mutually satisfactory methods for problem resolution at the lowest possible level as the optimum, with a procedure to escalate problem resolution through the appropriate chain-of-command, as deemed necessary.

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

Arrowhead Regional Medical Center 400 N. Pepper Avenue
Colton, CA 92324
Attn: ARMC Chief Executive Officer

Fivos, Inc.
8 Commerce Ave.
West Lebanon, NH 03784
Attn

Notice shall be deemed communicated two (2) County working days from the time of mailing if mailed as provided in this paragraph.

11.15 Governing Law and Venue. Except where preempted by federal law, this Agreement shall be governed by and construed in all aspects in accordance with the laws of the State of Delaware without regard to principles of conflicts of laws.

11.16 Addendum. If Business Associate is using hosted cloud computing services for any part of the services hereunder, the terms of the Business Associate Addendum for Cloud Services, attached as Exhibit A, shall apply and are hereby incorporated as though fully set forth herein.

11.17 Entire Agreement. This Agreement, including all Exhibits and other attachments, which are attached hereto and incorporated by reference, and other documents incorporated herein, represents the final, complete and exclusive agreement between the parties hereto. Any prior agreement, promises, negotiations or representations relating to the subject matter of this Agreement not expressly set forth herein are of no force or effect. This Agreement is executed without reliance upon any promise, warranty or representation by any party or any representative of any party other than those expressly contained herein. Each party has carefully read this Agreement and signs the same of its own free will.

11.18 This Agreement 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 Agreement. The parties shall be entitled to sign and transmit an electronic signature of this Agreement (whether by facsimile, PDF or other mail 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 Agreement upon request.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their authorized representatives, effective upon the Effective Date above.

San Bernardino County on behalf of
Arrowhead Regional Medical Center [COVERED ENTITY]

By: _____

Name: Dawn Rowe

Title: Chair, Board of Supervisors

Date: _____

Fivos, Inc. [BUSINESS ASSOCIATE]

By: _____

Name: Katie Emerson

Title: _____

Date: _____

EXHIBIT A

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 San Bernardino County on behalf of Arrowhead Regional Medical Center ("County") and Business Associate (also hereinafter referred to as "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.

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 upon request and no more than once annually.

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 ,upon written request not more than twice per calendar year, provide the County with report of audit logs specifically related to the County's Data, including user access, data creation, modification, and deletion. Such reports shall be provided at no cost to the County. For the avoidance of doubt, the County shall not have direct access to Contractor's internal security toolsets or infrastructure.
d) Contractor assumes responsibility for the security and confidentiality of the Data under its control.
e) 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 by this Contract and/or the underlying services agreement..

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 actual Data loss or unplanned loss of access to Data exceeding forty-eight (48) hours, Contractor shall notify the County by via mass electronic notification (email or maintenance page)Contractor shall provide such notification within twenty-four (24) hours after Contractor confirms such a disaster or catastrophic failure. In the notification, Contactor shall inform the County of:

1) The status of the investigation in the Recovery Point Objective (24 hours) and the estimated timeframe of data potentially affected (e.g. hours since last successful backup);
2) General efforts Contractor has taken to restore the SaaS service; and
3) Estimated timelines for service restoration, if known.
4) Formal reporting regarding the scope of Data loss will be provided via mass notification to client contacts once the system is complete and Contractor has verified the integrity of the backup restoration.

b) 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.

c) Contractor shall conduct an investigation of the disaster or catastrophic failure and shall share the summary report of the investigation findings with the County as it relates specifically to County Data. The Investigation shall be conducted solely by the Contractor; however, Contractor shall cooperate with reasonable requests for information from the County or law enforcement as required by law.

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

a) **In lieu of individual inspections,** Contractor shall provide the County, upon written request and subject to non-disclosure obligations, a copy of its most recent **SOC 2 Type 2 report and/or HITRUST certification summary**.

b) **Contractor does not permit third-party vulnerability scanning or penetration testing by the County on Contractor's production systems.** To ensure control efficacy, Contractor maintains a robust vulnerability management program and conducts annual third-party penetration tests. Contractor shall provide a **letter of attestation** or an executive summary of its most recent third-party penetration test results upon request.

c) In the event of a **confirmed** Data Breach affecting County Data, Contractor will, at its own cost, perform a third-party penetration test against the specific environment or application area affected by the breach. Any additional third-party audits required by the County following an event shall be **at the County's sole expense** and subject to a mutually agreed-upon scope that protects the proprietary information of Contractor and its other customers.

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 three (3) business days 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. DATA SEPARATION: Data must be logically separated 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.