_____

PROFESSIONAL SERVICES AGREEMENT

FOR

ECONSULT AND REFERRAL MANAGEMENT SOFTWARE SOLUTION

BETWEEN

COUNTY OF SAN BERNARDINO
ON BEHALF OF
ARROWHEAD REGIONAL MEDICAL CENTER

AND

SAFETY NET CONNECT, INC.
_____

PROFESSIONAL SERVICES AGREEMENT
ARROWHEAD REGIONAL MEDICAL CENTER

This Professional Services Agreement ("Agreement") is made and entered into by and between the County of San Bernardino, a political subdivision organized and existing under the constitution and the laws of the State of California, on behalf of Arrowhead Regional Medical Center ("COUNTY"), and Safety Net Connect, Inc**.,** a California corporation ("CONTRACTOR"). COUNTY is a political subdivision of the State of California operating a hospital or surgery center.

RECITALS

WHEREAS, COUNTY is in need of the professional services offered by CONTRACTOR; and

WHEREAS, CONTRACTOR has offered evidence of having the relevant specialized training and/or experience and/or knowledge and is interested in providing the scope of work as set forth herein, including any attachments hereto; and,

WHEREAS, County previously entered into a Memorandum of Understanding (Agreement No. 18-135) ("MOU") in which, IEHP, COUNTY and Riverside University Health System collectively agreed to adopt eConsult and where IEHP agreed to fund the "Initial Term" of the Multi-County eConsult Initiative ("MCeI") through March 20th, 2020; and,

WHEREAS, COUNTY now desires to contract directly with the CONTRACTOR for the eConsult services provided under the MOU;

NOW THEREFORE in consideration of the mutual promises, covenants and conditions hereinafter contained, and in the following exhibits or attachments attached hereto and incorporated herein by this reference:

ATTACHMENT A – SCOPE OF SERVICES- GENERAL
ATTACHMENT A-2-SCOPE OF SERVICES- IMPLEMENTATION
ATTACHMENT B – SCHEDULE OF FEES
ATTACHMENT C – OWNERSHIP INFORMATION
ATTACHMENT D – BUSINESS ASSOCIATE AGREEMENT
ATTACHMENT E – SAAS AGREEMENT
ATTACHMENT H – DATA SEGREGATION AND ACCESS CONTROL ADDENDUM

The Parties hereto mutually agree as follows:

1. **SERVICES**

   A.   Subject to the terms and conditions of this Agreement, CONTRACTOR shall provide the services necessary to perform in a complete, skillful and professional manner all those services described in Attachments A and A-2 ("Scope"). CONTRACTOR agrees to maintain any applicable professional license(s) as

required by law at all times while performing services under this Agreement.

B. Other than as specifically indicated in Attachment A, CONTRACTOR will not utilize the services of any subcontractors in providing the services required hereunder without COUNTY's prior written approval. CONTRACTOR shall request approval by submitting a written description of the services to be subcontracted. If approved by COUNTY, CONTRACTOR shall remain the prime contractor for the services and be responsible for the conduct and performance of each approved subcontractor. All references to CONTRACTOR in this Agreement in the context of providing services, where applicable, will also include CONTRACTOR's approved subcontractors.

C. CONTRACTOR, or its agents or subcontractors, shall not perform any services outside the United States of America without COUNTY's prior written consent. In the event CONTRACTOR is in breach of this Section, COUNTY shall have, in its sole discretion, the right to immediately terminate this Agreement.

2. COMPENSATION

A. COUNTY shall compensate CONTRACTOR for the services set forth in the Scope, upon approval of a properly presented invoice for services. Payment shall be made "net-60" terms from the date of receipt of a complete invoice.

B. COUNTY shall make payments to CONTRACTOR as outlined in Attachment B. CONTRACTOR shall submit invoices to COUNTY for authorized services within thirty (30) days of the month of the rendered service. Invoices from CONTRACTOR must be received by COUNTY no later than ninety (90) days from the month wherein the services were rendered; invoices submitted after ninety (90) days from the month of services are not eligible for reimbursement.

C. Other than as stated on Attachment B, price increases will not be permitted during the Agreement term. If applicable, annual increases shall not exceed the Consumer Price Index- All Consumers, All Items - Riverside- San Bernardino- Ontario, CA areas and be subject to satisfactory performance review by COUNTY and approved (if needed) for budget funding by the Governing Board.

D. The total compensation payable under this Agreement shall not exceed One Million Five Hundred Seventy Thousand dollars ($1,570,000.00). In no event shall compensation exceed this amount without a written amendment to this Agreement authorizing such increase in total compensation payable to CONTRACTOR. CONTRACTOR agrees to monitor its costs at all times and provide COUNTY forty-five (45) days' written notice if CONTRACTOR becomes aware that it may exceed the total compensation authorized pursuant to this Section.

E. It is expressly agreed between the parties that payment to CONTRACTOR does not constitute or imply acceptance by COUNTY of any portion of the CONTRACTOR's work.

F.　It is mutually agreed and understood that the obligations of COUNTY are contingent upon the availability of state and federal funds. In the event that such funds are not forthcoming for any reason, this Agreement is rendered null and void, and COUNTY shall immediately notify CONTRACTOR in writing. This Agreement shall be deemed terminated and of no further force and effect immediately on COUNTY's notification to CONTRACTOR. In the event of such termination, CONTRACTOR shall be entitled to reimbursement of costs for services rendered in accordance with this agreement up to the date of termination.

3.　DISALLOWANCE

In the event CONTRACTOR receives payment for services under this Agreement which are later disallowed for nonconformance with the terms and conditions herein, CONTRACTOR shall refund the disallowed amount to COUNTY within thirty (30) days of COUNTY's written request. COUNTY retains the option to offset the amount disallowed from any payment due to CONTRACTOR under this Agreement, or under any other contract or agreement between CONTRACTOR and COUNTY.

4.　TERM AND TERMINATION

A.　Term of Agreement. This Agreement shall be effective as of March 1, 2020 ("Effective Date") and shall continue in effect through February 28, 2025 ("Term") unless earlier terminated in accordance with the provisions of Paragraph B of Section 4 of this Agreement. This Agreement shall automatically expire on March 21, 2025.

B.　Termination.

1)　Termination for Convenience. COUNTY may terminate this Agreement, for convenience, upon thirty (30) days' written notice delivered in accordance with Section 21 (NOTICES).

2)　Termination for Cause. Should COUNTY determine that there is a basis for termination for cause, such termination shall be effected upon five (5) days' written notice to CONTRACTOR in accordance with Section 21 (NOTICES).

3)　Immediate Termination. Immediate termination shall be available to the non-defaulting party, as specified below, by providing written notice in accordance with Section 21 (NOTICES).

i. COUNTY may immediately terminate this Agreement upon COUNTY's determination that CONTRACTOR has engaged in a fraudulent activity against COUNTY or its health plan members.

ii. If CONTRACTOR is excluded, terminated, or suspended from

participation in any state or federal health care program, including, without limitation, appearing on the federal List of Excluded Individuals/Entities (LEIE), the Medi-Cal Suspended and Ineligible Provider List (SIPL), or the System for Award Management (SAM). CONTRACTOR understands that COUNTY is prohibited from paying CONTRACTOR for any services rendered on or after the date of exclusion.

    iii. Pursuant to any provision of this Agreement which expressly authorizes immediate termination.

    4) <u>Effect of Termination</u>.

        i. Upon expiration or termination of this Agreement for any reason, CONTRACTOR shall promptly:

        a. Furnish to COUNTY all documents related to services rendered under this Agreement, including without limitation, copies of work papers, schedules or other work products related to this Agreement that do not include contractor's intellectual property.

        b. On a pro rata basis, repay all fees and expenses paid in advance for any fees and expenses, including licensing fees, paid in advance for any Services which have not been provided.

        c. Provide reasonable cooperation and assistance to COUNTY in transitioning the Services to an alternate service provider.

        ii. Unless otherwise provided herein, the rights and obligations of any party which by their nature extend beyond the expiration or termination of this Agreement, shall continue in full force and effect, notwithstanding the expiration or termination of this Agreement. This includes, without limitation, the following provisions: DISALLOWANCE, INDEMNIFICATION, LIMITATION OF LIABILITY, WORK PRODUCT AND INTELLECTUAL PROPERTY, CONFIDENTIALITY, GOVERNING LAW; and VENUE.

5. **INDEMNIFICATION**

    A. CONTRACTOR shall indemnify, and hold harmless COUNTY, directors, officers, employees, agents and representatives (individually and collectively hereinafter referred to as "Indemnitees") from liability, loss, settlement, claim, demand, and expense of any kind, arising out of the performance of services or the omission of any required act under the Agreement (and as noted in Attachment A), of the CONTRACTOR, its officers, employees, subcontractors, agents or representatives. CONTRACTOR shall defend the Indemnitees in any claim or action based upon any such alleged acts or omissions, at its sole expense, which shall include all costs and fees, including, but not limited to, attorney fees, cost of investigation, defense,

and settlement or awards.

It is not the intent of the parties that the provisions of this Section and the provisions of the Indemnification provision in Attachment D shall be in conflict. In the event of any conflict, the Indemnification provisions in Attachment D shall be interpreted to relate only to matters within the scope of the HIPAA Business Associate Agreement.

B.   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 CONTRACTOR'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.

C.   CONTRACTOR's obligation hereunder shall be satisfied when CONTRACTOR has provided to COUNTY the appropriate form of dismissal relieving COUNTY from any liability for the action or claim involved.

D.   The specified insurance limits required in this Agreement shall in no way limit or circumscribe CONTRACTOR's obligations to indemnify and hold harmless the Indemnitees herein from third party claims.

6.   <u>LIMITATION OF LIABILITY</u>

Without affecting the indemnification obligations set forth in this Agreement, in no event shall either party be liable for consequential, indirect, or incidental damages, including, without limitation, lost profits, arising out of the services provided under this Agreement.

7. **INSURANCE**

Without limiting or diminishing CONTRACTOR's obligation to indemnify or hold COUNTY harmless, CONTRACTOR shall procure and maintain or cause to be maintained, at its sole cost and expense, the following insurance coverage during the term of this Agreement.

A. <u>Workers' Compensation/Employer's Liability</u> **-** 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 CONTRACTOR and all risks to such persons under this Ageement. If CONTRACTOR has no employees, it may certify or warrant to 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. <u>Commercial General Liability</u> **-** CONTRACTOR shall carry General Liability Insurance covering all operations performed by or on behalf of 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. <u>Vehicle Liability</u> **-** 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 CONTRACTOR is transporting one 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 CONTRACTOR owns no autos, a non-owned auto endorsement to the General Liability policy described above is acceptable.

D. <u>Professional Liability</u> **-** a limit of liability not less than $1,000,000 per occurrence and $2,000,000 annual aggregate 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. CONTRACTOR shall ensure continuous coverage for such length

of time as necessary to cover any and all claims (i.e. appropriate Tail Coverage for coverage written on claims made basis, etc.).

E. Cyber and Privacy Liability - Cyber Liability Insurance with limits of no less than $1,000,000 for each occurrence or event with an annual aggregate of $5,000,000 covering claims involving privacy violations, information theft, damage to or destruction of electronic information, negligent, 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. The below referenced coverage is required only if any products and/or services related to professional services or information technology (including hardware and/or software) are provided to COUNTY under this Agreement for such length of time as necessary to cover any and all claims.

1) Privacy & Network Liability: $1,000,000
2) Internet Media Liability: $1,000,000
3) Business Interruption & Expense: $1,000,000
4) Data Extortion: $1,000,000
5) Regulatory proceeding: $1,000,000
6) Data Breach Notification & Credit Monitoring: $1,000,000

F. 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.

G. If insurance coverage is provided on a "claims made" policy, the "retroactive date" shall be shown and must be before the date of the state 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.

H. General Insurance Provisions – All lines.

1) Insurance to be placed with insurers with a current A. M. BEST rating of not less than A: VIII (A:8) unless otherwise approved by COUNTY Risk Management.

2) CONTRACTOR must declare any deductibles or self-insured retentions ("SIRs") for insurance coverage required to be approved by COUNTY. Should any deductibles or SIRs be unacceptable to COUNTY, COUNTY may require CONTRACTOR to: 1) reduce or eliminate such deductibles or SIRs; 2) provide proof of ability to pay such required fees/expenses within the retention or deductible; and 3) procure a bond which guarantees

payment of losses and related investigations, claims administration, and defense costs and expenses.

3) CONTRACTOR shall furnish COUNTY with either 1) original Certificate(s) of Insurance or amendatory endorsements effecting coverage as required herein, or 2) if requested by COUNTY, provide original certified copies of policies including all Endorsements and all attachments thereto, showing such insurance is in full force and effect. Further, CONTRACTOR shall provide no less than thirty (30) days' written notice to COUNTY prior to any material modification, cancellation, expiration or reduction in coverage of such insurance. In the event that any policy of insurance required under this Agreement does not comply with the requirements, is not procured, or is canceled and not replaced, COUNTY has the right but not the obligation or duty to cancel this Agreement or obtain insurance if it deems necessary and any premiums paid by COUNTY will be promptly reimbursed by CONTRACTOR or COUNTY payments to CONTRACTOR will be reduced to pay for COUNTY purchased insurance. **CONTRACTOR shall not commence operations until COUNTY has been furnished original Certificate(s) of Insurance and endorsements.**

4) CONTRACTOR's insurance shall be construed as primary insurance, and COUNTY's insurance shall not be construed as contributory. CONTRACTOR shall require the carriers of required coverages to waive all rights of subrogation against COUNTY, its officers, employees, agents, volunteers, contractors and subcontractors. All general or auto liability insurance coverage provided shall not prohibit CONTRACTOR and CONTRACTOR'S employees or agents from waiving the right of subrogation prior to a loss or claim. CONTRACTOR hereby waives all rights of subrogation against COUNTY. All policies, except for Worker's Compensation, Errors and Omissions and Professional Liability policies shall contain additional endorsements naming COUNTY and its officers, employees, agents and volunteers as additional named insured with respect to liabilities arising out of the performance of services hereunder. The additional insured endorsements shall not limit the scope of coverage for COUNTY to vicarious liability but shall allow coverage for 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 2010.11 85.

5) CONTRACTOR shall pass down the insurance obligations contained herein to all tiers of subcontractors working under this Agreement.

6) The insurance requirements contained in this Agreement may be met with a program(s) of self-insurance acceptable to COUNTY.

7) CONTRACTOR agrees to notify COUNTY of any claim by a third party

or any incident or event that may give rise to a claim arising from the performance of this Agreement.

8) 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 CONTRACTOR and COUNTY or between COUNTY and any other insured or additional insured under the policy.

9) Insurance requirements are subject to periodic review by COUNTY. The COUNTY Director of Risk Management or designee is authorized, but not required, to reduce, waive or suspend any insurance requirements whenever COUNTY determines that any of the required insurance is not available, is unreasonably priced, or is not needed to protect the interests of COUNTY. In addition, if the Director 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 COUNTY, inflation, or any other item reasonably related to the COUNTY'S risk.

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

11) Any failure, actual or alleged, on the part of 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 County.

12) CONTRACTOR agrees to provide insurance set forth in accordance with the requirements herein. If CONTRACTOR uses existing coverage to comply with these requirements and that coverage does not meet the specified requirements, CONTRACTOR agrees to amend, supplement or endorse the existing coverage to do so.

8. **AVAILABILITY OF CONTRACT TERMS TO PUBLIC AGENCIES "PIGGYBACK CLAUSE".** Intentionally blank

9. **WORK PRODUCT AND INTELLECTUAL PROPERTY**

COUNTY acknowledges that all proprietary and intellectual property rights, title and interest, including copyright, in and to the original and copies of the Application Modifications, Application Software, Replacement Products, Source Code, System

Operating Software, and System Software elements that are provided originally by CONTRACTOR and not COUNTY, and the Documentation provided to COUNTY pursuant to this Agreement other than Third Party Software (which shall remain the property of the applicable third party, subject to COUNTY'S License), and any changes or modifications thereto are and shall remain the exclusive property of CONTRACTOR (hereinafter "Contractor Materials"), with all such Application Modifications, Application Software, Replacement Products, System Operating Software, and System Software being subject to the License granted to COUNTY pursuant to the SaaS agreement.

COUNTY releases all proprietary and intellectual property rights, title and interest, including copyright, in and to all Interfaces, Baseline Customizations and Additional Customizations developed pursuant to this Agreement ("Application Modifications") to CONTRACTOR, subject to CONTRACTOR'S incorporation of said Application Modifications into the Application Software in perpetuity and subject to CONTRACTOR'S provision of Maintenance and Support Services for the Application Software, as required by this Agreement, including (Scope of Work), inclusive of such Application Modifications and any Updates and Version Releases to Application Software, to COUNTY in exchange for COUNTY's full consideration therefore.

All User Data and other information entered into the System, including and any and all updates or modifications to User Data shall be deemed the COUNTY'S Confidential Information, as that term is defined in Paragraph 3.0 (Confidentiality) of Exhibit A (Additional Terms & Conditions) to this Agreement. Upon any expiration or termination of this Agreement, and continuously throughout the Term, CONTRACTOR will make available to and otherwise provide Authorized Users with a complete copy of the most recent back up of the User Data in a mutually agreed upon, commercially standard format that is compatible with the User's then existing systems, and will make commercially reasonable efforts to assist the User in the transition of such User Data as reasonably requested by the requesting User. Upon request, CONTRACTOR, within ten (10) days of termination, certify in writing its compliance with this Paragraph to the requesting User. During the term of the Agreement, COUNTY or its Users may make suggestions or provide input regarding the functions or features of the System. This Agreement shall not be construed as granting any ownership rights in CONTRACTOR to any User Data or any other COUNTY Confidential Information. The User Data shall not be used by CONTRACTOR for any purpose other than as required under this Agreement, nor shall the User Data or any part of the User Data be disclosed, sold, assigned, leased or otherwise disposed of to third parties by CONTRACTOR or commercially exploited or otherwise used by or on behalf of CONTRACTOR, its officers, directors, employees, subcontractors or agents.

CONTRACTOR will not retain any User Data for any period longer than necessary for CONTRACTOR to fulfill its obligations under this Agreement. As soon as CONTRACTOR no longer needs to retain such User Data in order to perform its duties under this Agreement, CONTRACTOR will, at COUNTY'S direction and in COUNTY"S

sole discretion, promptly return to each User and destroy or erase all originals and copies of such User Data.

10. **LICENSE/ACCESS GRANT**

CONTRACTOR hereby grants to COUNTY a worldwide, non-exclusive license to access and use the System and Work, including any related Documentation (hereinafter "License"), by all Authorized Users in accordance with the scope set forth in this paragraph and subject to the Service as a Software Agreement, attached hereto as Exhibit E, for COUNTY's business purposes during the term specified in Term).

11. **OFFICERS, OWNERS, STOCKHOLDERS AND CREDITORS**

On an annual basis, CONTRACTOR shall identify the names of the following persons and update such names by providing COUNTY with thirty (30) days written notice of any changes in the information of such persons by listing them on Attachment C:

A.   CONTRACTOR officers and owners who own greater than 5% of the CONTRACTOR;

B.   Stockholders owning greater than 5% of any stock issued by CONTRACTOR;

C.   Major creditors holding more than 5% of any debts owed by CONTRACTOR;

12. **NONDISCRIMINATION**

This Agreement hereby incorporates by reference the provisions of *Title 2, California Code of Regulations, Sections 11105 et seq.*, as may be amended from time to time. CONTRACTOR agrees to comply with the provisions of *Title 2, CCR, Sections 11105 et seq.*, and further agrees to include this Nondiscrimination Clause in any and all subcontracts to perform services under this Agreement.

13. **CONFLICT OF INTEREST**

CONTRACTOR shall have no interest, and shall not acquire any interest, direct or indirect, which will conflict in any manner or degree with the performance of services required under this Agreement.

14. **PROTECTED HEALTH INFORMATION ("PHI")**

CONTRACTOR further agrees to the provisions of the HIPAA Business Associate Agreement, attached hereto in Attachment D, and incorporated herein by this reference.

15. **CONFIDENTIALITY**

A.   Each Party receiving Confidential Information (a "Receiving Party") hereunder, as defined below, shall hold the Confidential Information in strict confidence and use and access the Confidential Information only as is necessary for the performance of this Agreement. Each Receiving Party may only disclose Confidential Information to its employees and third party consultants who have a bona fide need

to know. Receiving Party shall not otherwise disclose Confidential Information without the prior written consent of the other party (the "Disclosing Party") or as required by law.

B.   Confidential Information means any technical, financial, trade secrets, or any information the Disclosing Party has received from others, including personal information, which it is obligated to treat as confidential or proprietary, including without limitation, any and all ideas, techniques, processes, methods, systems, cost data, computer programs, formulas, work in progress, customers/members, business plans, and other business information. Confidential Information shall not include any information that:

1)   Is or becomes available to the public (other than through any act or omission of Receiving Party);

2)   Is required to be disclosed pursuant to an applicable law, subpoena, or court order, provided that the Receiving Party notifies the Disclosing Party to allow Disclosing Party to protect its interests, if desired;

3)   Is independently developed by the Receiving Party without access to any Confidential Information of the Disclosing Party;

4)   Is lawfully known by the Receiving Party at the time of disclosure or otherwise lawfully obtained by a third party with no obligation of confidentiality.

16.   PUBLIC ENTITY STATUS; BROWN ACT/PUBLIC RECORDS ACT

The parties hereby acknowledge and agree that COUNTY is a local public entity of the State of California subject to the Brown Act, *California Government Code Sections 54950 et seq.*, and the Public Records Act, *California Government Code Sections 6250 et seq.*

17.   COMPLIANCE WITH LEGAL AND REGULATORY REQUIREMENTS

A.   General. The parties shall observe and comply with all applicable county, state and federal laws, ordinances, rules and regulations now in effect, subsequently amended or hereafter enacted. The parties shall further observe and comply with all applicable executive orders, directives, requirements (including state and/or federal contract requirements), and standards by any organization having jurisdiction over COUNTY or any Authorized User to regulate the delivery of health care services. This shall include applicable accrediting organizations. All the aforementioned items are hereby made a part hereof and incorporated herein by reference.

18.   AUDIT RIGHTS

A.   CONTRACTOR understands that COUNTY is a county managed provider regulated by entities, including without limitation, DMHC, DHCS, and the Centers

for Medicare and Medicaid Services. To the extent CONTRACTOR is identified as a subcontractor for which COUNTY is required to do oversight due to its legal and/or contractual obligations to such regulatory agencies, the following provisions shall apply:

1) Maintenance of Records. CONTRACTOR will maintain complete and accurate books, records and documentation, including audited financial statements prepared in accordance with generally accepted accounting procedures and practices, to sufficiently and properly reflect the services provided and CONTRACTOR's direct and indirect costs invoiced in the performance of the Agreement. The retention period for such books and records shall be for a period of ten (10) years or as otherwise stated in the Attachments to this Agreement.

2) Records Subject to Inspection. All books, records, documents, and other materials maintained by CONTRACTOR and relating to the Agreement will be subject, at reasonable times during regular business hours and upon thirty (30) days prior written notice, to examination, inspection, copying, or audit by authorized COUNTY personnel. The parties agree that books, records, documents, and other evidence of accounting procedures and practices related to CONTRACTOR's cost structure, including overhead, general and administrative expenses, and profit factors will be excluded from COUNTY's review.

3) Subcontracts. CONTRACTOR will incorporate into any subcontracts the records retention and review requirements of this Section.

19. **EXCLUSION/DEBARMENT LISTS**

A. CONTRACTOR represents that it, and the employees and consultants engaged under this Agreement, are not excluded, debarred, or suspended individuals/entities under any exclusion or debarment list relating to state or federal health care programs, including the Federal List of Excluded Individuals/Entities (LEIE), System for Award Management, and the Suspended and Ineligible Provider List. CONTRACTOR warrants that such status shall be maintained throughout the term of this Agreement.

B. CONTRACTOR understands that if CONTRACTOR or any of its employees or consultants engaged under this Agreement is excluded, debarred or suspended and appears on any such list COUNTY is required to terminate this Agreement immediately, and prohibits COUNTY from paying CONTRACTOR for any services rendered on or after the date of exclusion. Should CONTRACTOR be in receipt of payment for services rendered after the exclusion date, CONTRACTOR agrees to submit a refund of such fees upon written notice by COUNTY. COUNTY expressly reserves its right to recoup payment of such fees under Section 3 (DISALLOWANCE).

20. **NOTICES**

Other than correspondences for which email communication is expressly reserved pursuant to the terms of this Agreement, all notices required or contemplated by this Agreement shall be delivered to all those listed below in the manner and at the addresses set forth below or to such other address(es) as the parties may hereafter designate, in writing. Such notices will be deemed given if sent by certified United States mail or commercial courier, at the time of receipt confirmed by corresponding documentation.

COUNTY: CONTRACTOR:

William L. Gilbert   Chris Cruttenden
Director   President
ARMC   Safety Net Connect, Inc.
400 North Pepper Avenue   4600 Campus Drive, Suite 101
Colton CA 92324   Newport Beach, CA 92660
                                          949-399-5382
                                          ccruttenden@netchemistry.com

ARMC (CC):
Arrowhead Regional Medical Center
Attn: Joy Davis /Maria Tucci
400 North Pepper Avenue
Colton CA 92324

21. **SEVERABILITY**

In the event any provision of this Agreement is determined by any court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions of this Agreement will continue in full force and effect.

22. **WAIVER**

A waiver by a party of any breach of any one (1) or more of the terms of this Agreement shall not be construed to be a waiver of any subsequent or other breach of the same term or of any other term herein.

23. **INDEPENDENT CONTRACTOR**

It is understood and agreed that the relationship between the parties is an independent contractor relationship. Neither party, including its officers, agents, employees or subcontractors, shall be considered to be employees of the other, nor entitled to any benefits payable to such employees, including Workers ' Compensation Benefits. None of the provisions of this Agreement shall be construed to create a relationship of agency, representation, joint venture, ownership, control or employment between the parties other than that of independent parties contracting for the purposes of effectuating this Agreement.

24. GOVERNING LAW; VENUE

A.   The provisions of this Agreement shall be construed in accordance with the laws of the State of California, excluding its conflicts of law provisions.

B.   The provisions of the Government Claims Act (*California Government Code Sections 900 et seq.*) must be followed for any disputes under this Agreement.

C.   All actions and proceedings arising in connection with this Agreement shall be tried and litigated exclusively in the state or federal (if permitted by law) courts located in the County of San Bernardino, State of California.

25. FORCE MAJEURE

Each party shall be excused from performing hereunder to the extent that it is prevented from performing as a result of any act or event which occurs and is beyond the reasonable control of such party, including, without limitation, acts of God, war, or action of a governmental entity; provided that the affected party provides the other party with prompt written notice thereof and uses all reasonable efforts to remove or avoid such causes.

26. ASSIGNMENT

A party may not sell, assign, transfer, or otherwise convey this Agreement without the prior express written consent of the other party. Any attempted assignment of this Agreement not in accordance with this Section shall be null and void.

27. CHANGE IN CONTROL

CONTRACTOR must obtain COUNTY's written consent prior to CONTRACTOR entering into (i) any transaction or series of related transactions (including, but not limited to, any reorganization, merger, or consolidation) that results in the transfer of 50% or more of the outstanding voting power; or (ii) sale of all or substantially all of the assets of the CONTRACTOR to another person or entity. In the event CONTRACTOR fails to obtain COUNTY's prior written consent, COUNTY shall have the option to terminate this Agreement immediately.

28. ALTERATION AND/OR AMENDMENT

No alteration, amendment, or variation of the terms of this Agreement shall be valid unless made in writing and signed by the parties hereto, and no oral understanding or agreement not incorporated herein, shall be binding on any of the parties hereto. Only the County of San Bernardino Board of Supervisors or designee may authorize any alteration or revision of this Agreement on behalf of COUNTY. Notwithstanding the foregoing, amendments required due to legislative, regulatory or other legal authority do not require the prior approval of CONTRACTOR and shall be deemed effective immediately (or such other time frame as required by law or regulation) upon CONTRACTOR's receipt of notice. Notice of amendments required by law, regulation or other legal authority shall be given as provided in Section 21 (NOTICES).

29. __ENTIRE AGREEMENT__

This Agreement, including all attachments, which are hereby incorporated in this Agreement, supersedes any and all other agreements, promises, negotiations or representations, either oral or written, between the parties with respect to the subject matter and period governed by this Agreement and no other agreement, statement or promise relating to this Agreement shall be binding or valid.

30. __COUNTERPARTS; SIGNATURES__

This Agreement may be executed in separate counterparts, each of which shall be deemed an original, and all of which shall be deemed one and the same instrument. The parties' faxed signatures, and/or signatures scanned into PDF format, shall be effective to bind them to this Agreement.

31. __COUNTERPARTS; SIGNATURES__

If there is a conflict between the documents comprising the Agreement, the following order of precedence shall apply:
a) Applicable federal and State laws, regulations and policies;
b) The Business Associate Agreement (Attachment D);
c) The terms and conditions in the body of this Agreement;
d) The terms of the Attachments (except Attachment D) and/or other documents attached to this Agreement, provided that no order of precedence shall be applied among such Attachments and/or other documents;
e) The Documentation

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, the parties hereto certify that the individuals signing below have authority to execute this Agreement on behalf of their respective organizations, and may legally bind them to the terms and conditions of this Agreement, and any attachments hereto. The parties have signed this Professional Services Agreement as set forth below.

COUNTY OF SAN BERNARDINO

► _____

Curt Hagman, Chairman, Board of Supervisors

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

SAFETY NET CONNECT, INC.

_____

By ► _____
         (Authorized signature – sign in blue ink)

Name _____
        CHRIS CRUTTENDEN

Title _____
       PRESIDENT

Dated: 12-13-2019

FOR COUNTY USE ONLY

Approved as to Legal Form	Reviewed for Contract Compliance	Reviewed/Approved by Department
► _____	► _____	► _____
County Counsel		
Date _____	Date _____	Date _____

17

ATTACHMENT A

SCOPE OF SERVICES-GENERAL

CONTRACTOR shall provide implementation services according to what is outlined below. Further, the eConsult System will function according to the following requirements:

1. Business Requirements: CONTRACTOR's integrated eConsult Platform shall meet or exceed the business requirements outlined below:

    A.   Meet the needs of eConsult integration within the following systems:
         1) ARMC – Meditech, currently
            – Epic, upon installation and go live
    B.   Seamless integration with the EHR by providing both data and system integration including Single Sign On (SSO), with the eConsult Platform, a session and user authentication service that permits the provider and staff to use their EHR or organization workstation login credentials (e.g., username and password) to access eConsult with patient context as a means of providing ease of use by end-users.
    C.   System shall be capable of supporting systems with and without standard interfaces and/or Application Program Interfaces.
    D.   Customization shall be provided at the direction of COUNTY within the defined Scope of Work.
    E.   Unique patient or member search capabilities within the application.
    F.   Providing patient context when initiating an eConsult outside of an EHR system that will include eConsult ordering via the EHRs and resulting of the eConsult back to the Order in the EHR for that encounter
    G.   Users can view their work list and status of active list items in summary.
    H.   Support for mandated data elements within eConsult request templates.
    I.   Clinically pertinent questions associated with the eConsult requests are in a structured format.
    J.   Clinical and workflow guidelines are available to reduce the potential for missing information within the eConsult to the specialist.
    K.   Information requirements can be customized on a specialty basis, ensuring clinically pertinent information is complete, reducing the potential for specialists to request additional information, causing delays and unnecessary loopbacks.
    L.   Discrete data elements are integrated, uploaded, faxed or pasted from between the EHR and the eConsult solution to better inform specialists, dependent on the capabilities for interoperability provided by the EHR vendor.
    M.   Specialist correspondence that includes the ability to attach information or documentation for the PCP to review within the EHR, or the eConsult portal e.g. study results or education information.
    N.   PCP's can access a specific list of specialists with whom they communicate on a frequent basis.
    O.   Users can locate specialists when requesting an eConsult using a list of available providers or provide automation to qualified and responsive providers, eliminating the need for PCP's to select specialists.

P. Inactive specialists can be identified and made unavailable within the application where routing is not automated.

Q. PCP initiates eConsult. PCP and specialist resolve eConsult. If eConsult resolves in a face-to-face, this will be automatically authorized through the health plans electronic authorization portal MedHOK. eConsult shall contain the necessary data and information to process authorization. CONTRACTOR will work with COUNTY to define the necessary data and information that is required and will use best efforts to interface with COUNTY'S MedHOK authorization system to provide the necessary data and information.

R. Provides CPT code assignment for claims billing purposes.

S. Solution shall support Code Sets, including but not limited to: ICD-9, ICD10, LOINC, SNOMED, NCPDP, CPT, NPI.

T. Dynamic lookup list of CPT and ICD10 codes.

U. Three (3) bi-directional HL7 interfaces, to be determined by customer, shall be provided at no additional cost identified per Attachment A and the fee schedule for interfaces. COUNTY shall not be required to purchase any additional interfaces.

V. Ability to flag for increased urgency where necessary.

W. Specialist can flag eConsult request as inappropriately routed and can return to sender.

X. PCP's can provide ratings-related feedback associated with the communications process with specialty providers.

Y. PCP's can easily understand which eConsults are closed versus those that remain active or open.

Z. Upon completion of clinically pertinent question and attachment of document, eConsult can be routed to a Specialist reviewer without further decision making by PCP.

AA. Upon specialist request for face-to-face with patient, solution provides electronic referral request automation.

BB. SaaS hosting within the United States of America.

CC. Ability to manage sudden surges in demand without adversely affecting system use.

DD. Planned growth in demand shall be proactively managed so that system use is not adversely affected.

EE. High availability to include 100% failover capabilities along every system component. Each piece of hardware will have an uninterruptible power supply and network connectivity.

FF. Incident protection and detection software shall be utilized to scan the network for vulnerabilities.

GG. All data shall be encrypted at rest and transmission level with encryption & security measures meeting SOC2 standards. (SOC 2)

HH. System shall have backup and recovery capabilities in place that ensure prompt and complete data recovery.

II. eConsult shall be accessible on commonly used platforms, including but not limited to, Windows 7, Mac OSX, Windows IE, Mozilla Firefox, Google Chrome, Android.

JJ. Accessibility and use via any supported device capable of web browsing.

Mobile Devices:
Internet Explorer – 8 through 11
Firefox – Current Version or One previous
Chrome – Current Version or one

Supported   Devices:
Workstation Devices:
IE - Current Version or one previous
Firefox – Current Version or one previous
Chrome – Current Version or one previous
   Safari   –   5   through   6

KK. The eConsult system must integrate with EHR in place, with the ability to populate data fields into eConsult in order to avoid duplicate entry of information include ADMIT, DISCHARGE, TRANSFER ("ADT"), documentation, orders and results

LL. Access control maintained through a policy agreed to by COUNTY.

MM. Capability of use with Primary Care, Specialty Care, and other ancillary departments

NN. Ability to be used by external providers to initiate eConsults and track referrals.

OO. Automated notification / list of eConsults in task-based queues.

PP. Ability to communicate with all participating clinics (primary to specialty care).

QQ. Note tracking that can be viewed at all points of the eConsult status.

RR. Status capabilities/reports of the stage the eConsult is in.

SS. Built in specialty protocol/criteria, guidelines, e-forms, pre-eConsult questions as provided by customer.

TT. Bi-directional communication capability for providers within eConsult, including mailbox capabilities.

UU. Built in quality and utilization tools to track responses, authorizations and eConsult and referral wait times based on provided data from the customer.

VV. Ability to review, create, request and complete forms; ability to save forms to document library.

WW. Use of clinical guidelines/checklists, as provided by COUNTY, associated with initiating specialist communication in order to ensure appropriateness of the request and sufficient detail/supporting documentation are submitted to the specialist reviewer.

XX. Solution shall not require any prerequisite software, or layered or middleware.

YY. Solution shall have controls in place that ensure the accuracy of information throughout its lifecycle.

ZZ. Solution shall adhere to all HIPAA standards for security.

AAA. Integration to Active Directory as identified in the request for proposals, one for COUNTY.

BBB. System shall maintain locations/equipment sufficient to provide backup capability in the event of a loss of power.

CCC. CONTRACTOR shall maintain well-documented security infrastructure.

DDD. Audit trail logs shall be provided upon the request of COUNTY.

EEE. Solution shall comply with infrastructure standards certification, including International Standards Organization/International Electrical Commission.

FFF. Delegation of user provisioning administration shall be provided to COUNTY.

2. Reporting Requirements:

A. Administrators shall have the ability to run standard ad-hoc reports using various filters to drill down to specific items, as well as the ability to run visual analytic reports that allow them to identify data trends and drill down to individual data elements for their patient populations.

B. Standard reporting measures include, but are not limited to:
1) Number of specialty touches/population referred to specialty care.
2) Demographics of patients who received an eConsult.
3) Percentage of patients who received specialty expertise via eConsult.
4) Local Specialist use of eConsult versus CONTRACTOR network specialist dependency.
5) eConsult management
6) Number of specialties offering eConsult and what they are.
7) Unclosed loop by PCP.
8) Unclosed loop by specialist.
9) Average time to eConsult response.
10) Number of eConsults requiring additional information.
11) eConsult rating statistics.

3. EHR Integration and Interface Requirements:

A. Solution will provide data & workflow integration with COUNTY EHRs and if needed with HIE systems using predefined interfaces. Data integration will include ADT, SSO, Patient demographics. Documentation, Ordering and Resulting.
1) **EHR Integration with eConsult platform**
   i. **eConsult will access and store:**
   ii. patient demographics (e.g., First Name, Last Name, Birthday, Address, Email, Phone, Cell, and/or other fields to be defined)
   iii. provide patient context (e.g., MRN, ICD-10 code, Specialty, Primary Care Provide, notes, and other clinical documentation to be defined)
   iv. provide eligibility information on patient
   v. (See Interface Requirements, 3. G.) System will upload clinical documentation from EHR to eConsult.
2) **Launch eConsult platform from within the EHR**
   i. *(See Interface Requirements, 3. E.) Providers can access the eConsult platform from within their EHR via an imbedded link or other user interface method);* and
3) **Push final eConsult note back to the EHR** for that patient encounter, including, but not limited to:
   i. clinical notes,
   ii. eConsult close codes,
   iii. PCP and specialist dialog, etc.
      (See Business Requirements, 1. F) Providing patient context when initiating an eConsult outside of an EHR system that will include: eConsult ordering via the EHRs; and resulting of the eConsult back to the EHR for that encounter.
4) **System will upload** clinical documentation from EHR to eConsult (See

Interface Requirements, 3. G.).

5) **eConsult notifications in the EHR:** Ability for the EHR to be notified when an eConsult has been initiated, in progress, and completed (See Interface Requirements, 3. Y.).

B. Solution will interface with legacy systems, repository systems, foreign systems, modalities and devices.
C. Patient demographics are interfaced real-time.
D. Provider names list is kept up to date via import to eConsult using the batch process to update, add and/or disable providers to eConsult.
E. Solution will share laboratory results from EHR within the eConsult application with specialist based on recent encounters of patient history.
F. Providers can access the eConsult solution from within their EHR and, if needed, the HIE system.
G. Users can upload clinical documentation from EHR within eConsult.
H. Users can upload image files with eConsult.
I. The following data types and code sets are supported and can be processed interactively include, but not limited to: ASCII, BLOB, EBCDIC, LOINC, ORU, TIFF, hex16, hex32, printable, raw, signed binary and unsigned binary.
J. Error monitoring will provide an alert subsystem which will generate alert message(s) when data interfaces fail.

4. Software Functionality Requirements:

A. Work queues
B. Alerts for changes in status
C. Storage of patient demographics including history
D. Ability to upload documents
E. Ability to upload pictures
F. Ability to upload films or xrays
G. Ability to store video
H. Ability to stream video
I. Ability to attached faxes and scans to patient records
J. Ability to add customizable clinical guidelines that can interface with multiple organizations
K. Ability to export into PDF of XTML summary of eConsult or communication
L. Ability to interface with existing referral/authorization applications
M. Ability to interface with existing scheduling application
N. Open architecture
O. Web-based
P. Single sign-on capability
Q. Ability to create multiple roles
R. Hosted model
S. Readily scalable
T. Modular
U. Ability to interface with EHR including via HL7

V.   Ability for non-clinical staff messaging (administrative)

W.   Ability to create reports, including but not limited to:
1) Total eConsults generated and received
2) Total eConsults in dialog
3) Total eConsults closed
4) Total eConsults summary
5) Total scheduled eConsult
6) Total PCP activity
7) User list
8) SR billing report
9) Patient demographics

X.   Ability for discrete abstraction of data type for custom reporting.

Y.   Ability for the EHR to be notified when an eConsult has been done so that information that resides in the eConsult solution can be available to HIM for release of information to the patient or law enforcement when requested.

5.   CONTRACTOR shall collaborate with the Executive Sponsor to plan the post implementation and expansion management for the ongoing successful use of the eConsult Platform. The post implementation plan will include step by step tasks, resources necessary and a plan outline.

6.   SaaS Service Level Agreement

A.   Dedicated hosting services' target availability percentage is 99.99 percent.

B.   All measurements based on a thirty (30) day measurement period.

C.   Server availability of 99.9% standard, which equates to four (4) hours per month of downtime. This down time will include unscheduled maintenance windows.

D.   Mean time to respond to P1 trouble reports shall be fifteen (15) minutes. Calls that are not answered directly will receive a call back within fifteen (15) minutes of the time the message is recorded.

E.   Mean time to restore service shall be two (2) hours. Any server outage shall be resolved and the service will be brought back on-line within two (2) hours.

F.   Mean time to repair shall be four (4) hours. The cause of the server outage will be corrected within four (4) hours.

7.   Support Services Service Level Agreement

A.   Definitions:
1) "Resolve" is defined herein, with respect to an incident, that a workaround or fix with respect to such incident has been implemented by CONTRACTOR and accepted by COUNTY.
2) "Respond" is defined herein, with respect to an incident, that CONTRACTOR has notified COUNTY of such Incident and commenced steps to resolve such incident.
3) "Scheduled Uptime" is defined herein as twenty four (24) hours each day, seven (7) days per week, excluding regular maintenance windows between

the hours of 10:00 p.m. and 2:00 a.m. Pacific time on Saturdays. Notwithstanding Scheduled Outages, CONTRACTOR shall ensure that the system software and hosting services remains available during the foregoing maintenance windows to the extent reasonably practicable.

   4) "Server" is defined herein as the server(s) on which the system software and hosting services will be hosted.

B.   Priority Level 1 (P1): Major Business Impact. "Priority 1" or "P1" means an Incident that causes complete loss of the system software or hosting services to customer's production environment such that work cannot reasonably continue and no workarounds to provide all of the functionality of the system software and hosting services required under the Agreement are possible or cannot be implemented in time to minimize the impact on customer's business. P1 Incidents have one or more of the following characteristics: (i) a large number of users cannot access all of the system software and hosting services, (ii) critical functionality is not available, (iii) the system software and hosting services or any portion thereof cannot function because a vital feature is inoperable, or (iv) data cannot be secured, backed up, recovered or processed as required by the Agreement.

C.   Priority Level 2 (P2): Significant Business Impact. "Priority 2" or "P2" means an incident that results in a significant loss of the system software and hosting services to COUNTY'S production environment such that processing can proceed in a restricted fashion but performance is significantly reduced and/or operation of the system software and hosting services or any portion thereof is considered severely limited and no workaround to provide the affected functionality is possible or cannot be implemented in time to minimize the impact on COUNTY'S business. P2 Incidents have one or more of the following characteristics: (i) one or more deficiencies or other errors causing the system software or hosting services to fail, but restart or recovery is possible, (ii) severely degraded performance, or (iii) some important functionality is unavailable, yet the system software and hosting services continues to operate in a restricted fashion.

D.   Priority Level 3 (P3): Minor Business Impact. "Priority 3" or "P3" means an incident that results in minimal loss of the system software and hosting services or any portion thereof to COUNTY'S production environment such that the impact of the incident is minor or an inconvenience, such as requiring a manual bypass to restore product functionality. P3 Incidents have one or more of the following characteristics: (i) a Deficiency or other error for which there is a workaround that is acceptable to COUNTY, (ii) there is minimal performance degradation, or (iii) a deficiency or other error that requires manual editing of configuration or script files to address an incident.

E.   Priority Level 4 (P4): No Business Impact. "Priority 4" or "P4" means an incident that causes no loss of the system software and hosting services and in no way impedes COUNTY'S use of the system software and hosting services in accordance with the Agreement. P4 Incidents have one or more of the following characteristics:

(i) an update for which there is workaround that is acceptable to COUNTY, or (ii) a documentation error.

F.   Service Monitoring and Management: CONTRACTOR shall perform continuous monitoring and management of the system software and hosting services to optimize availability of system. Included within the scope of this paragraph is the proactive monitoring of the server and all service components of CONTRACTOR's firewall for trouble on a 7 day by 24 hour basis, and the expedient restoration of components when failures occur within service outages. CONTRACTOR shall maintain redundancy in all key components such that outages are less likely to occur due to individual component failures. CONTRACTOR will monitor "heartbeat" signals of all servers, routers and leased lines, and HTTP availability of the system software and hosting services, by proactive probing at 30-second intervals 24 hours a day using an automated tool. If a facility does not respond to a ping-like stimulus, it shall be immediately checked again. When CONTRACTOR receives a "down" signal, or otherwise has knowledge of an outage or incident (including, without limitation, any failure in the server, system and /or system software) CONTRACTOR shall immediately work on expedient restoration of failures.

G.   Service Levels

    1) Availability: At a minimum, the system software and hosting services shall be available for the percentage of the time each month of the term as set forth on the Service Level Matrix.

    2) Response Time: Response Time shall be calculated for each Incident occurring in a calendar month as the total minutes commencing from the time when CONTRACTOR becomes aware of a P1, P2, P3, or P4 Incident, whether by automated alarm or otherwise, until CONTRACTOR responds to each such incident. CONTRACTOR shall track each P1, P2, P3 and P4 incident, and the time required to respond to each such incident. The response time service level is set forth on the Service Level Matrix available in the SaaS agreement.

    3) Resolution Time: Resolution Time shall be calculated for each incident occurring in a calendar month as the total minutes commencing from the time when CONTRACTOR becomes aware of a P1, P2, P3, or P4 Incident, whether by automated alarm or otherwise, until CONTRACTOR resolves each such incident as determined by COUNTY. CONTRACTOR shall track each P1, P2, P3 and P4 Incident and the time required to resolve each such incident. The Resolution Time Service Level is set forth on the Service Level Matrix.

    i.   Non-Emergency Outage Incidents: CONTRACTOR shall track each non-emergency outage incident that occurs outside of the regularly scheduled maintenance windows. The non-emergency outage incidents service level is set forth on the Service Level Matrix.

    4) Tracking: CONTRACTOR shall be responsible for measuring and

monitoring Service Level performance at a level of detail sufficient to verify CONTRACTOR's compliance with the applicable service levels.

5) Data Return: CONTRACTOR shall return all subscriber data, including all user data and PHI, in accordance with the requirements of this Agreement not later than the number of days after COUNTY'S request as set forth on the Service Level Matrix.

6) Service Level Audits: COUNTY or its designee shall have the right to audit CONTRACTOR's measurement, monitoring and tracking on all Service Levels, including providing COUNTY with access to the data used by CONTRACTOR to calculate its performance against the Service Levels and the measurement and monitoring tools and procedures utilized by CONTRACTOR to generate such data for purposes of audit and verification.

H.   Issue Escalation: Issues regarding eConsult and/or the site availability shall be considered CONTRACTOR's highest priority. If the issue is deemed to originate with the eConsult and/or the site hardware or software, the support representative will promptly escalate the issue to CONTRACTOR's Engineering Group. If eConsult and/or the site is unavailable for longer than twenty (20) continuous minutes, all affected subscribers will be notified via email to the relevant Use Administrators. Issues regarding general usage, bug reports, documentation, etc., will be handled using the escalation procedure below.

1) Trouble tickets: will be tracked using an integrated multi-level support ticket system. A trouble ticket is generated by the user that includes the time, date, class/severity, and a chronology of the problem as it is managed through a ticket response list. If an issue is deemed to originate with the software application, a support representative will escalate the issue to a Second Level Support request.

2) First Level Support: is provided via the eConsult system. First Level support is also provided by a specified COUNTY support representative and includes answering general service questions via the support ticket system. If the issue cannot be answered, it will be escalated within a reasonable period of time to Second Level support.

3) Second Level Support: consists of senior support representatives and support management; these individuals will make every reasonable attempt to answer the problem during the same business day. COUNTY will be notified by email and informed of the estimated time of resolution. Follow-up messages are sent as deemed necessary to ensure COUNTY is properly informed.

4) After hours emergency service line: is used for critical application errors or website unavailable issues. This support consists of senior support representatives; these individuals will make every reasonable attempt to resolve the problem ASAP. Emergency issues, limited to unavailability of the eConsult and/or the Site, may be reported 7x24 (seven days per week; 24 hours per day) by calling CONTRACTOR's Emergency Hotline at (949) 260-9397. Support by email may also be sent to

support@SafetyNetConnect.com.

I.   DEFINITIONS:
1) "CPT code" means Current Procedural Terminology code, a medical code set maintained by the American Medical Association through the CPT Editorial Panel.
2) "EHR" means COUNTY electronic health records system.
3) "HIE" means health information exchange.
4) "PCP" means primary care physician.

ATTACHMENT A-2

SCOPE OF SERVICES – IMPLEMENTATION DELIVERABLES

CONTRACTOR shall meet or exceed the implementation and go live requirements according to this ATTACHMENT A-2.

1. Implementation shall include up to ten all specialties, the following primary care sites, initially one (1) San Bernardino County Sherriff's Department and six (6) ARMC, to provide consults with specialists for managed care patients for the purpose of facilitation an automatically authorized specialty care visit.

2. Any subsequent phases will include all clinic and primary care sites, replacing existing referral systems and process with a unified eConsult and care management process and system. Implementation will be coordinated with the IEHP Multi County eConsult Initiative Project Team as identified in the RFP.

3. CONTRACTOR shall maintain effective, timely, and thorough communication with COUNTY using an established project communication plan which has been submitted to and approved by COUNTY prior to the commencement of work.

4. CONTRACTOR shall follow quality assurance processes and plans based on a plan submitted to and approved by COUNTY, prior to the commencement of work.

5. CONTRACTOR shall follow a reporting plan based on a plan submitted to and approved by COUNTY, prior to the commencement of work.

6. CONTRACTOR shall follow processes and plans submitted to and approved by COUNTY, prior to the commencement of work.

7. CONTRACTOR shall develop and complete all deliverables under this Agreement based on a plan submitted to and approved by COUNTY prior to the commencement of work.

8. Completion of "Scope Deliverables" (as defined below) is contingent on receiving the minimum necessary deliverables from COUNTY in a timely manner. Project plan/timelines will be updated upon receipt of approved business requirements.

9. Implementation the eCRM Module is contingent on receiving the minimum necessary deliverables from COUNTY, in a timely manner. Project plan/timelines will be updated upon receipt of approved business requirements.

A. Scope Deliverables

Scope Deliverables: Overview of Process for Additional eConsult Enhancements

Future enhancements to the eConsult platform are based upon an interactive process between CONTRACTOR and COUNTY to refine the specifications of each enhancement.

CONTRACTOR will work with COUNTY to refine the requirements for future eConsult platform enhancements. CONTRACTOR utilizes an interactive process to develop a Build Requirements Document (BRD) that the Client will review and provide "sign-off" prior to any modification work begins. Such BRD will present an estimation of hours and cost budget. Along with the BRD, CONTRACTOR shall provide a project timeline. A typical project timeline is set forth as follows:

1. Finalize Business Requirements and a SOW document   1-2 weeks
2. Development and Internal testing Completion   12 weeks
3. Client Completes User Acceptance Testing   4 weeks
4. Client Reports finding to technical team   2 days
5. Technical Team reviews/Fixes Findings   3 days
6. Client re-tests updated sites   1 week
7. Client Signs off on Testing   1 day
8. Push to Demo and Production/ Training and Go-Live   2 days

** Note - Timeline dependencies resulting from external, non-CONTRACTOR resources may alter the expected duration of the development and internal testing efforts.

Deliverables for anticipated future enhancements are set forth below. Utilizing the standard CONTRACTOR approach, the specific items will be collaboratively refined and presented in a BRD. Upon completion of the BRD, a timeline shall be set forth based upon the work effort agreed upon. For planning and budgeting purposes, based on the information available, we have provided estimated budget cost and targeted completion timelines.

1. **Scope Deliverable 1: eCRM Module Enhancements**
   a. eCRM Module enhancements and configuration per requirements
   b. Future enhancements to the eCRM system identified by COUNTY will undergo collaborative scope development and cost estimation by COUNTY and CONTRACTOR. Rates for future enhancements will be per the hourly fee schedule in Attachment B.
   c. CONTRACTOR shall develop and complete all deliverables under this scope of work based on a plan submitted to and approved by COUNTY prior to the commencement of work.

ATTACHMENT B

SCHEDULE OF FEES

SAFETY NET CONNECT, INC.

1. CONTRACTOR shall invoice COUNTY electronically for eConsult and Referral Management Software Solution fees to COUNTY's Accounts Payable Office at. Each invoice shall cite the CONTRACTOR's name, address, and remit to address, description of the work performed, the time period covered by the invoice, and the amount of payment requested.
2. CONTRACTOR requests for payments and reimbursements must comply with the requirements set forth in Attachment A. Requests for services shall be on an as needed basis.
3. The consideration to be paid to CONTRACTOR, as provided herein, shall be in full payment for all CONTRACTOR Services and expenses incurred in the performance hereof, including travel and per diem. CONTRACTOR shall adhere to COUNTY'S Travel Management Policy (8-02 and 08-02SP1) when travel is pursuant to this Agreement and for which reimbursement is sought from COUNTY. In addition, CONTRACTOR is encouraged to utilize local transportation services, including but not limited to, the Ontario International Airport.
4. Compensation. COUNTY shall compensate CONTRACTOR as follows:
   a. Fees. As specified below, compensation under this Agreement is for the implementation and licensing of the eConsult System for COUNTY and the COUNTY participants ("Participants"). Except as expressly provided herein, COUNTY shall not be responsible for any other charges or expenses for Participant's to access the system, use or transition away from the Services.
   b. Implementation fees shall be paid in accordance with the below payment schedule.

IMPLEMENTATION FEES		
Payment Description	**Payment Date**	**Payment**
eCRM Module Customization	Upon "First Productive Use"	$50,000.00
Total IMPLEMENTATION FEES		**$50,000.00**

   c. License fees shall be paid in accordance with the below payment schedule. COUNTY is financially responsible for all License fees for Months 1-60 ("License Period").

LICENSE FEES					
License fees for Months 1-24					
Description	**Amount**	**Note:**	**Unit**	**Per month**	**Annual Fees**
Base SaaS License	$15,000.00 / per Month	The $15,000.00 fee is a fixed monthly fee. The fee is independent of	1	$15,000.00	$180,000.00

		number of sites or users; See SaaS Agreement. For unlimited Users at each licensed site.			
Originating Site Fee	$500.00 / per Site	Originating site is where a provider initiates an eConsult, similar to a referring site, limited to primary care providers	**7 sites**	$3,500.00	$42,000.00
eCRM Module SaaS Fee	$6,000 per month	The $6,000.00 fee is a fixed monthly fee. The fee is independent of number of sites or users; See SaaS Agreement.; For Unlimited users and sites	**1**	$6,000.00	$72,000.00
Total					**$294,000.00**

*Fees to implement any additional "sites" added within COUNTY's operated outpatient network shall not exceed $500/per "Site"

5. Total compensation, under this AGREEMENT as listed below, for sixty (60) months will not exceed one million five hundred and twenty thousand ($1,520,000.00).

TOTAL FEES		
Description	**Unit**	**Payment Amount per Year (12 months)**
Total BASE Service as a Software "SaaS" License Fee	$15,000.00 per month for 12 months	$180,000.00
Total Site Use License Fee for 7 sites per month	$3,500.00 per month for 12 months	$42,000.00
eCRM Module SaaS Fee	$6,000 per month for 12 months	72,000.00
Total SaaS and Lice Fees Annually		**$294,000.00**
eCRM One-time Development Fee	Per SOW #1	$50,000.00
TOTAL Fees Year 1		**$344,000.00**

Fee Schedule	
Year 1: (March 1, 2020 – February 28, 2021)	**$344,000.00**
Year 2: (March 1, 2021 – February 28, 2022)	$294,000.00
Year 3: (March 1, 2022 – February 28, 2023)	$294,000.00
Year 4: (March 1, 2023 – February 28, 2024)	$294,000.00
Year 5: (March 1, 2024 – February 28, 2025)	$294,000.00
TOTAL (60 months)	**$1,520,000.00**

d. Additional rates for customizations and consulting services on an as-needed basis shall be paid in accordance with the below payment schedule. However, any additional customizations and technical assistance require COUNTY's prior written approval.

Safety Net Connect Professional Hourly Rates	
Resource	Hourly Rate
Architect	$250.00
Database Administrator	$200.00
Designer	$125.00
Engineer	$200.00
Web Developer	$125.00
Multimedia	$175.00
Project Manager	$150.00
System Administrator	$175.00
Test Engineer	$150.00

Safety Net Connect Training and Consulting Service Rates	
Resource	Hourly Rate
Client Project Manager	$150.00
Technical Workflow Manager	$175.00
Technical Workflow Analyst	$150.00

e. **Termination of Participation in eConsult System within Months 1-60**. Upon thirty (30) days written notice of intent to terminate its use of the eConsult System ("Notice"), CONTRACTOR shall reimburse COUNTY for (i) any prepaid License fees; and (ii) any prepaid fees for implementation for services to the extent that such services have not been performed by the date of Notice. In the event such termination is due to CONTRACTOR'S failure to deliver the requirements in the Scope, as defined in Attachments A and A-2, CONTRACTOR shall reimburse COUNTY for the total amount of Implementation fees paid for the Participant's implementation.

ATTACHMENT C

<u>OWNERSHIP INFORMATION</u>

Contractor's Name: _____

Tax Identification Number (TIN): _____

Address: _____

City: _____ **State:** _____ **Zip:** _____

Phone: _____

President: _____ **Contact Person:** _____

Person Signing Contract: _____

Broker Representative: _____

Please circle below how your organization is legally organized:

- **Sole Proprietorship**

- **Partnership (LLC, etc.)**

- **Corporation**
  - o **Privately Held Company***
  - o **Publicly Traded Company**
  - o **Non-Profit Entity**

- **Government Agency**

- **Other (please indicate):** _____

_____   _____
Authorized Signature   Date

HIPAA BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (BAA) supplements and is made a part of the contract ("Contract") by and between the County of San Bernardino on behalf of Arrowhead Regional Medical Center (hereinafter "Covered Entity") and Safety Net Connect Inc. (hereinafter "Business Associate"). This BAA is effective as of the effective date of the Contract.

RECITALS

WHEREAS, Covered Entity ("CE") wishes to disclose certain information to Business Associate ("BA") pursuant to the terms of the Contract, which may include Protected Health Information ("PHI"); and

WHEREAS, CE and BA intend to protect the privacy and provide for the security of the PHI disclosed to BA pursuant to the Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("HITECH Act"), their implementing regulations, and other applicable laws; and

WHEREAS, The Privacy Rule and the Security Rule require CE to enter into a contract containing specific requirements with BA prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, sections 164.314, subdivision (a), 164.502, subdivision (e), and 164.504, subdivision (e) of the Code of Federal Regulations ("C.F.R.") and contained in this Agreement; and

WHEREAS, Pursuant to HIPAA and the HITECH Act, BA shall fulfill the responsibilities of this Agreement by being in compliance with the applicable provisions of the HIPAA Standards for Privacy of PHI set forth at 45 C.F.R. sections 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards), 164.316 (Policies and Procedures and Documentation Requirements), and, 164.400, et seq. and 42 United States Code ("U.S.C.") section 17932 (Breach Notification Rule), in the same manner as they apply to a CE under HIPAA;

NOW THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties agree as follows:

A.   Definitions
Unless otherwise specified herein, capitalized terms used in this BAA shall have the same meanings as given in the Privacy Rule, the Security Rule, the Breach Notification Rule, and HITECH Act, as and when amended from time to time.
1. 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 as further described in California Civil Code section 1798.82.
2. Business Associate (BA) 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. section 17921 and 45 C.F.R. section 160.103.

3. Covered Entity (CE) 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. section 160.103.

4. Designated Record Set shall have the same meaning given to such term under 45 C.F.R. section 164.501.

5. Electronic Protected Health Information (ePHI) means PHI that is maintained in or transmitted by electronic media as defined in the Security Rule, 45 C.F.R. section 164.103.

6. Individual shall have the same meaning given to such term under 45 C.F.R. section 160.103.

7. 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. Parts 160 and 164, subparts A and E.

8. Protected Health Information (PHI) shall have the same meaning given to such term under 45 C.F.R. section 160.103, limited to the information received from, or created or received by Business Associate from or on behalf of, CE.

9. Security Rule means the regulations promulgated under HIPAA by HHS to protect the security of ePHI, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, subparts A and C.

10. 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. section 17932, subdivision (h).

B. Obligations and Activities of BA

1. Permitted Uses and Disclosures

BA may disclose PHI: (i) for the proper management and administration of BA; (ii) to carry out the legal responsibilities of BA; (iii) for purposes of Treatment, Payment and Operations (TPO); (iv) as required by law; or (v) for Data Aggregation purposes for the Health Care Operations of CE. Prior to making any other disclosures, BA must obtain a written authorization from the Individual.

If BA discloses PHI to a third party, BA must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such PHI will be held confidential as provided pursuant to this BAA and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify BA of any breaches of confidentiality of the PHI, to the extent it has obtained knowledge of such breach. [42 U.S.C. section 17932; 45 C.F.R. sections 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)]

2. Prohibited Uses and Disclosures

i. BA shall not use, access or further disclose PHI other than as permitted or required by this BAA and as specified in the attached Contract or as required by law. Further, BA shall not use PHI in any manner that would constitute a violation

of the Privacy Rule or the HITECH Act. BA shall disclose to its employees, subcontractors, agents, or other third parties, and request from CE, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder.

 ii. BA shall not use or disclose PHI for fundraising or marketing purposes.

 iii. BA 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).)

 iv. BA shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CE and as permitted by the HITECH Act (42 U.S.C. section 17935(d)(2); and 45 C.F.R. section 164.508); however, this prohibition shall not affect payment by CE to BA for services provided pursuant to this BAA.

3. Appropriate Safeguards

 i. BA shall implement appropriate safeguards to prevent the unauthorized use or disclosure of PHI, including, but not limited to, administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of the PHI BA creates, receives, maintains, or transmits on behalf of the CE, 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).]

 ii. In accordance with 45 C.F.R. section 164.316, BA 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.

 iii. BA 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 CE'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 BA under this BAA.

4. Subcontractors

BA shall enter into written agreements with agents and subcontractors to whom BA provides CE's PHI that impose the same restrictions and conditions on such agents and subcontractors that apply to BA with respect to such PHI, and that require compliance with all appropriate safeguards as found in this Agreement.

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

Every suspected and actual Breach shall be reported immediately, but no later than one (1) business day upon discovery, to CE's Office of Compliance, consistent with the regulations under HITECH Act. Upon discovery of a Breach or suspected Breach, BA shall complete the following actions:

 i. Provide CE'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 names and titles of each person allegedly involved;
d) Number of potentially affected Individual(s) with contact information; and
e) Description of how the Breach or suspected Breach allegedly occurred.

ii. Conduct and document a risk assessment by investigating without unreasonable 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 had access to the PHI;
c) Whether the PHI was actually acquired or viewed; and
d) The extent to which the risk to PHI has been mitigated.

iii. Provide a completed risk assessment and investigation documentation to CE'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 CE, additional information may be requested.
a) If BA and CE agree that 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 BA must provide CE with affected Individual(s) name and contact information so that CE can provide notification.

iv. Make available to CE and governing State and Federal agencies in a time and manner designated by CE 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 CE reserve the right to conduct its own investigation and analysis.

6. Access to PHI
To the extent BA maintains a Designated Record Set on behalf of CE, BA shall make PHI maintained by BA or its agents or subcontractors in Designated Record Sets available to CE for inspection and copying within ten (10) days of a request by CE to enable CE to fulfill its obligations under the Privacy Rule. If BA maintains ePHI, BA shall provide such information in electronic format to enable CE to fulfill its obligations under the HITECH Act. If BA receives a request from an Individual for access to PHI, BA shall immediately forward such request to CE.

7. Amendment of PHI
If BA maintains a Designated Record Set on behalf of the CE, BA shall make any amendment(s) to PHI in a Designated Record Set that the CE directs or agrees to, pursuant to 45 C.F.R. section 164.526, or take other measures as necessary to satisfy CE's obligations under 45 C.F.R. section 164.526, in the time and manner designated by the CE.

8. Access to Records

BA shall make internal practices, books, and records, including policies and procedures, relating to the use, access and disclosure of PHI received from, or created or received by BA on behalf of, CE available to the Secretary of HHS, in a time and manner designated by the Secretary, for purposes of the Secretary determining CE'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 CE upon request.

9.   Accounting for Disclosures
     BA, its agents and subcontractors shall document disclosures of PHI and information related to such disclosures as required by HIPAA. This requirement does not apply to disclosures made for purposes of TPO. BA shall provide an accounting of disclosures to CE or an Individual, in the time and manner designated by the CE. BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents or subcontractors for at least six (6) years prior to the request. At a minimum, the information collected and maintained shall include:
     i.   the date of disclosure;
     ii.   the name of the entity or person who received PHI and, if known, the address of the entity or person;
     iii. a brief description of PHI disclosed; and
     iv.   a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

10. Termination
     CE may immediately terminate this BAA, and any related agreements, if CE determines that BA has breached a material term of this BAA. CE may, at its sole discretion, provide BA an opportunity to cure the breach or end the violation within the time specified by the CE.

11. Return of PHI
     Upon termination of this BAA, BA shall return all PHI required to be retained by the BA or its subcontractors, employees or agents on behalf of the CE. In the event the BA determines that returning the PHI is not feasible, the BA shall provide the CE with written notification of the conditions that make return not feasible. Additionally, the BA must follow established policies and procedures to ensure PHI is safeguarded and disposed of adequately in accordance with 45 C.F.R. section 164.310, and must submit to the CE a certification of destruction of PHI. For destruction of ePHI, the National Institute of Standards and Technology (NIST) guidelines must be followed. BA further agrees to extend any and all protections, limitations, and restrictions contained in this BAA, to any PHI retained by BA or its subcontractors, employees or agents after the termination of this BAA, and to limit any further use, access or disclosures.

12. Breach by the CE
     Pursuant to 42 U.S.C. section 17934, subdivision (b), if the BA is aware of any activity or practice by the CE that constitutes a material Breach or violation of the CE's

obligations under this BAA, the BA must take reasonable steps to address the Breach and/or end eliminate the continued violation, if the BA has the capability of mitigating said violation. If the BA is unsuccessful in eliminating the violation and the CE continues with non-compliant activity, the BA must terminate the Agreement (if feasible) and report the violation to the Secretary of HHS.

13. Mitigation

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

14. Costs Associated to Breach

    BA 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 CE and shall not be reimbursable under this BAA at any time. CE shall determine the method to invoice the BA for said costs. Costs shall incur at the current rates and may include, but are not limited to the following:

    - Postage;
    - Alternative means of notice;
    - Media notification; and
    - Credit monitoring services.

15. Direct Liability

    BA may be held directly liable under HIPAA for impermissible uses and disclosures of PHI; failure to provide breach notification to CE; failure to provide access to a copy of ePHI to CE or individual; failure to disclose PHI to the Secretary of HHS when investigating BA's compliance with HIPAA; failure to provide an accounting of disclosures; and, failure to enter into a business associate agreement with subcontractors.

16. Indemnification

    BA agrees to indemnify, defend and hold harmless CE 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 BA, its officers, employees, agents and subcontractors, with respect to the use, access, maintenance or disclosure of CE's PHI, including without limitation, any Breach of PHI or any expenses incurred by CE in providing required Breach notifications.

17. Judicial or Administrative Proceedings

    CE may terminate the Contract, effective immediately, if (i) BA 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 BA has been joined that the BA has violated any standard or requirement of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws.

18. Insurance
In addition to any general and/or professional liability insurance coverage required of BA under the Contract for services, BA shall provide appropriate liability insurance coverage during the term of this BAA to cover any and all claims, causes of action, and demands whatsoever made for loss, damage, or injury to any person arising from the breach of the security, privacy, or confidentiality obligations of BA, its agents or employees, under this BAA and under HIPAA 45 C.F.R. Parts 160 and 164, Subparts A and E.

19. Assistance in Litigation or Administrative Proceedings
BA shall make itself, and any subcontractors, employees, or agents assisting BA in the performance of its obligations under the BAA, available to CE, at no cost to CE, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, 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 BA or its subcontractor, employee or agent is a named adverse party.

C. Obligations of CE
1. CE shall notify BA of any of the following, to the extent that such may affect BA's use, access, maintenance or disclosure of PHI:
    i. Any limitation(s) in CE's notice of privacy practices in accordance with 45 C.F.R. section 164.520.
    ii. Any changes in, or revocation of, permission by an individual to use, access or disclose PHI.
    iii. Any restriction to the use, access or disclosure of PHI that CE has agreed to in accordance with 45 C.F.R. section 164.522.

D. General Provisions
1. Remedies
BA agrees that CE shall be entitled to seek immediate injunctive relief as well as to exercise all other rights and remedies which CE may have at law or in equity in the event of an unauthorized use, access or disclosure of PHI by BA or any agent or subcontractor of BA that received PHI from BA.

2. Ownership
The PHI shall be and remain the property of the CE. BA agrees that it acquires no title or rights to the PHI.

3. Regulatory References
A reference in this BAA to a section in the Privacy Rule and Security Rule and patient confidentiality regulations means the section as in effect or as amended.

4. No Third-Party Beneficiaries
Nothing express or implied in the Contract or this BAA is intended to confer, nor shall

anything herein confer, upon any person other than CE, BA and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

5. <u>Amendment</u>
    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 BAA may be required to ensure compliance with such developments. The parties shall negotiate in good faith to amend this BAA when and as necessary to comply with applicable laws. If either party does not agree to so amend this BAA within 30 days after receiving a request for amendment from the other, either party may terminate the BAA upon written notice. To the extent an amendment to this BAA is required by law and this BAA 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 BAA automatically and without further action required by either of the parties. Subject to the foregoing, this BAA may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed and agreed to by BA and CE.

6. <u>Interpretation</u>
    Any ambiguity in this BAA shall be resolved to permit CE to comply with the Privacy and Security Rules, the HITECH Act, and all applicable patient confidentiality regulations.

7. Compliance <u>with State Law</u>
    In addition to HIPAA and all applicable HIPAA Regulations, BA acknowledges that BA and CE may have confidentiality and privacy obligations under State law, including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code §56, et seq. ("CMIA")). If any provisions of this BAA 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 BA shall comply with the more restrictive requirements.

8. Survival
    The respective rights and obligations and rights of CE and BA relating to protecting the confidentiality or a patient's PHI shall survive the termination of the Contract or this BAA.

EXHIBIT 1
Business Associate Addendum for Cloud Services

This Business Associate Addendum for Cloud Services is in addition to and made a part of the Business Associate Agreement ("BAA") entered into between the parties for the purpose of establishing terms and conditions applicable to the provision of hosted cloud computing services from Business Associate (BA) to the Covered Entity (CE). Capitalized terms shall have the same meaning as provided in the BAA.

1. DEFINITIONS:
    a) "Software as a Service (SaaS)" – The software delivery method that provides CE access to BA's software and its functions remotely as a Web-based service accessible from various CE devices through a thin client interface. CE 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 CE or CE's employees, agents and end users upload, create or modify using the SaaS. Data also includes user identification information, PHI, 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 BAA terms and/or applicable state or federal law.

2. SaaS AVAILABILITY: Unless otherwise stated in a Statement of Work (SOW):
    a) 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), CE 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, CE may terminate the contract for material breach.
    d) BA shall provide advance written notice to CE 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) 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), CE shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the SOW if CE is unable to access the Data as a result of:
        1) Acts or omissions of BA;
        2) Acts or omissions of third parties working on behalf of BA;
        3) Network compromise, network intrusion, hacks, introduction of viruses, disabling devices, malware and other forms of attack that can disrupt access to BA's server, to

the extent such attack would have been prevented by BA taking reasonable industry standard precautions;

    4) Power outages or other telecommunications or Internet failures, to the extent such outages were within BA'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, CE may terminate the contract for material breach.

4. DATA SECURITY:
  a) In addition to the provisions set forth in the BAA, BA shall certify to CE:
    1) The sufficiency of its security standards, tools, technologies and procedures in providing SaaS;
    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 BA's plan to correct any negative findings shall be made available to CE within thirty (30) business days of BA's receipt of such results.

  b) BA 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 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 CE's access to its Data.

  c) BA shall allow CE reasonable access to SaaS security logs, latency statistics, and other related SaaS security data under this Addendum and CE's Data, at no cost to CE.

  d) BA assumes responsibility for the security and confidentiality of the Data under its control.

  e) No Data shall be copied, modified, destroyed or deleted by BA other than for normal operation or maintenance of SaaS during the Addendum period without prior written notice to and written approval by CE.

  f) BA shall provide access to Data only to those employees, contractors and subcontractors who need to access the Data to fulfill BA's obligations under this Agreement. BA will ensure that, prior to being granted access to Data, staff who perform SaaS work 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 BAA; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

5. ENCRYPTION: BA 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 CE, and BA has a limited, non-exclusive license to access and use the Data as provided to BA solely for performing its obligations under the BAA. 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 BA 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 the BAA, or upon notice of termination of the BAA, BA shall assist CE in extracting and/or transitioning all Data in the format determined by CE ("Transition Period").
   b) The Transition Period may be modified in the SOW or as agreed upon in writing by the parties in an amendment.
   c) During the Transition Period, SaaS and Data access shall continue to be made available to CE without alteration.
   d) BA agrees to compensate CE for damages or losses CE incurs as a result of BA's failure to comply with this section.
   e) Unless otherwise stated in the SOW, the BA shall permanently destroy or render inaccessible any portion of the Data in BA's and/or subcontractor's possession or control following the expiration of all obligations in this section. Within thirty (30) days, BA shall issue a written statement to CE confirming the destruction or inaccessibility of CE's Data.
   f) CE, at its option, may purchase additional transition services as agreed upon in the SOW.

9. DISASTER RECOVERY/BUSINESS CONTINUITY: Unless otherwise stated in the SOW:
   a) In the event of disaster or catastrophic failure that results in significant Data loss or extended loss of access to Data, BA shall notify CE by the fastest means available and also in writing. BA shall provide such notification within twenty-four (24) hours after BA reasonably believes there has been such a disaster or catastrophic failure. In the notification, BA shall inform CE of:
      i. The scale and quantity of the Data loss;
      ii. Actions BA has done or will do to recover the Data and mitigate any deleterious effect of the Data loss; and
      iii. Corrective actions BA has taken or will take to prevent future Data loss.
   b) If BA fails to respond immediately and remedy the failure, CE may exercise its options for assessing damages or other remedies.
   c) BA 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 or an SOW. Failure to do so may result in CE exercising its options for assessing damages or other remedies.
   d) BA shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with CE. CE and/or its authorized agents shall have the right to

lead (if required by law) or participate in the investigation. BA shall cooperate fully with CE, its agents and law enforcement.

10. EXAMINATION AND AUDIT: Unless otherwise stated in the SOW:
    a) Upon advance written request, BA agrees that CE or its designated representative shall have access to BA's SaaS operational documentation and records, including online inspections that relate to the security of the SaaS purchased or licensed by the CE.
    b) BA shall allow CE, 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:
        iv. Operating system/network vulnerability scans,
        v. Web application vulnerability scans,
        vi. Database application vulnerability scans, and
        vii. Any other scans to be performed by CE or representatives on behalf of CE.
    c) After any significant Data loss or Data Breach or as a result of any disaster or catastrophic failure, BA will at its expense have an independent, industry-recognized, CE-approved third party perform an information security audit. The audit results shall be shared with CE within seven (7) days of BA's receipt of such results. Upon BA receiving the results of the audit, BA will provide CE with written evidence of planned remediation within thirty (30) days and promptly modify its security measures in order to meet its obligations under this Addendum.

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

12. Insurance Requirements: BA 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 BA's records, information or data for reasons or activities that are not directly related to CE's business.

<div align="center">

ATTACHMENT E

SAAS AGREEMENT

</div>

SAAS AGREEMENT FOR ECONSULT AND REFERRAL MANAGEMENT SOFTWARE SOLUTION

This Agreement (the "Agreement") is made between Safety Net Connect, Inc., located at 4600 Campus Drive, Suite 101, Newport Beach, California 92660 ("Safety Net Connect"), and the County of San Bernardino on behalf of Arrowhead Regional Medical Center ("Subscriber") as of March 1. 2020 (the "Effective Date").

BACKGROUND

Safety Net Connect has developed systems consisting of software and services marketed under the trade name "ASP Modular Platform" or "AMP" to which it provides access on a subscription basis. These systems contain proprietary information, software code, intellectual property, and materials of Safety Net Connect, and may contain functionality and content licensed from third parties, and is hosted at the Safety Net Connect data centers with access provided over the World Wide Web. Subscriber wishes to obtain access to the AMP configuration(s) specified in Attachment A of the MASTER SERVICES AGREEMENT (MSA) ("SCOPE OF SERVICES") for its business use, and Safety Net Connect wishes to provide such access in accordance with the terms set forth below and in the MSA. In consideration of the mutual covenants and obligations set forth below, the parties agree as follows:

AGREEMENT

1. Definitions.

1.1. "Use Administrator" shall mean the Subscriber employee(s) designated by Subscriber to administer the use of AMP by Authorized Users

1.2. "Authorized User" means a Subscriber employee, client, or vendor who has received a valid Login Credential from the Use Administrator.

1.3. "Login Credential" shall mean the unique User ID with an associated password assigned to each Authorized User by the Use Administrator which permits access to AMP.

1.4. "World Wide Web" is the portion of the Internet which is the current mode of access to AMP which runs on the Safety Net Connect System.

1.5. "Safety Net Connect Content" means proprietary information, materials, databases and other content which is made available to Subscriber and each Authorized User through AMP except such documentation which is in the public domain.

1.6. "Safety Net Connect System" means the Safety Net Connect proprietary software, systems, processes, trade knowledge, intellectual property, and hardware configuration which generates, enables and serves AMP except such which is in the public domain. 1.7. "Site" means the location on the World Wide Web through which the Authorized Users may access AMP.

1.8. "Subscriber Data" means any proprietary information, data, text, and/or images provided by Subscriber to Safety Net Connect for implementation within AMP or that which is input or uploaded to AMP by an Authorized User.

1.9. "ASP Modular Platform" or "AMP" is comprised of the software and service features described in Attachment A of this Agreement which are made available to Subscriber and its Authorized Users

by Safety Net Connect via the World Wide Web, as such features and functionality may be modified from time to time as set forth below.

1.10. "Third Party Content" means certain content licensed to Safety Net Connect from third parties for display on AMP, including without limitation quotes, news, video and other content, as well as certain functionality which enables aspects of the Platform.

1.11. "Spam" means unsolicited email, soliciting emails, pseudo emails, impersonating emails, or other unwanted emails using our software to email addresses (persons) that have not joined your email list willfully or who have no previous relationship with Subscriber.

2. Subscriber Rights and Obligations.

2.1. Grant to Users. Subject to the terms of this Agreement, Safety Net Connect grants to Subscriber a non-exclusive, non- transferable, right and license (i) to access and use AMP with a validly-issued Login Credentials solely for Subscriber's business purposes; (ii) to access and use the Safety Net Connect Content and Third Party Content (collectively, the "Site Content") displayed on AMP solely for the Subscriber's business purposes; and (iii) to input, upload, download and otherwise use the Subscriber Data displayed on AMP without restriction. Subscriber may never use the system for sending Spam email under any circumstances.

2.2. Current Version/Upgrades/New Products. The parties acknowledge and agree that the term "AMP" or "ASP Modular Platform" as used in this Agreement shall include all functionality and services as described in Attachment A of this Agreement. From time to time Safety Net Connect may release a new version, enhancement or improvement ("Upgrade") to AMP that may be implemented at the Subscriber's discretion. Upgrades shall be licensed to Subscriber pursuant to the terms of this Agreement at no additional Subscription Fees. Upgrades are to be distinguished from "New Products" which shall mean and include, without limitation, features, functionality, and/or components that may be marketed as products separate from AMP, and may include products used in connection with AMP. The parties acknowledge and agree that Safety Net Connect may request additional fees (including, but not limited to, license, subscription and professional services fees) for Subscriber's use of such New Products, subject to the parties entering into a separate agreement covering terms of use and pricing for such New Products.

2.3 Link From Subscriber Site. INTENTIONALLY OMITTED.

2.4. Service Levels and Support. Safety Net Connect will use commercially reasonable efforts to host and maintain AMP and provide the Subscriber support according to the standards specified in Schedule A ("Service Levels And Subscriber Support").

2.5. Subscriber Data. Subscriber shall have the non- exclusive, non-transferable right to post and upload Subscriber Data to AMP. Subscriber represents and warrants to Safety Net Connect that any and all such Subscriber Data will not: (i) violate any federal, state, or local law or regulation; (ii) infringe any U.S. copyright, trademark or other proprietary right of any third party; (iii) in any way violate or infringe upon any party's privacy right, right of publicity or any other right of any person or entity; or (iv) contain any material which is unlawful, hateful, obscene, libelous, threatening or defamatory. Subscriber acknowledges that Safety Net Connect has no obligation to monitor the Subscriber Data, but, in the event that Safety Net Connect becomes aware that any item of Subscriber Data does or may violate the warranty and representation set forth in this Section 2.5, Subscriber agrees that Safety Net Connect shall have the right to remove such item pending resolution, and the parties agree to work together promptly and in good faith to remedy any such Subscriber Data issues. Standard volume of Subscriber Data to be stored on AMP may be limited as described in Schedule A.

2.6. Restrictions. AMP, the Site, the Platform and the Site Content shall only be used by Subscriber and its Authorized Users for Subscriber's or its Authorized Users' non-commercial business

purposes; and Subscriber agrees to use commercially reasonable efforts to ensure that neither AMP nor the Site Content is displayed outside the Site or distributed in any way to any third party not authorized hereunder to access or use same. Except as expressly authorized in this Agreement, Subscriber shall not rent, lease, sublicense, distribute, grant a security interest in, transfer, copy, reproduce, display, modify or timeshare AMP, the Site, the Platform or the Site Content or any portion thereof, or use such as a component of or a base for products or services prepared for commercial sale, sublicense, lease, access or distribution other than to or on behalf of the Authorized Users, or prepare any derivative work based on AMP, the Site, the Platform or the Site Content. Subscriber shall not knowingly allow any third party or unlicensed user or computer system to access or use AMP, the Site, the Platform or the Site Content. Subscriber agrees not to demonstrate or disclose the results of any testing or bench- marking of AMP, the Site, the Platform, or Site Content to any third party without Safety Net Connect's prior written permission, and such information will constitute the Confidential Information (as defined below in Section 9) of Safety Net Connect. Safety Net Connect reserves all rights not expressly granted to Subscriber. Subscriber agrees to take all commercially reasonable steps to protect AMP, the Site, the Platform and the Site Content from unauthorized access, copying or use. The parties acknowledge that Subscriber is a local government agency subject to the California Public Records Act. Subscriber agrees to notify Safety Net Connect of any request under such Act that might require disclosure of Confidential Information.

3. Fees and Payment. INTENTIONALLY OMITTED.

4. Use Administrator; Login Credential Protection.

4.1. Use Administrator. Promptly after the Effective Date, Subscriber shall designate an employee or various employees to serve as Use Administrator(s) for Subscriber. Subject to the terms of this Agreement, Safety Net Connect grants the Subscriber the non-transferable right and license to access and use AMP, including without limitation to assign and administrate Login Credentials to Authorized Users, to administer security profiles of Authorized Users, and to input data regarding the Authorized Users, and to upload Subscriber Data. Subscriber warrants and represents that each Authorized User will be assigned a unique Login Credential, and that no Login Credential will be shared or otherwise utilized by two or more individuals at any time.

4.2. Login Credential Protection. Subscriber shall be solely responsible for the security of the Login Credential issued to each Authorized User. Subscriber agrees to comply with industry standard procedures from time to time regarding obtaining and updating Login Credentials to AMP. Login Credentials are subject to cancellation or suspension by Safety Net Connect upon the misuse of any Login Credential by Subscriber or any Authorized User, Subscriber agrees to use commercially reasonable efforts to ensure that each Authorized User prevents any third party from obtaining his or her Login Credential, and Subscriber shall inform Safety Net Connect immediately of any actual or potential unauthorized access to a Login Credential or to AMP.

5. Proprietary Rights.

5.1. Safety Net Connect Rights. All right, title and interest in and to AMP, the Site, the Platform, the Site Content and the Safety Net Connect System and related documentation (including any corrections, updates, adaptations, enhancements thereto or authorized copies thereof) shall remain exclusively with Safety Net Connect and its licensors, as applicable. Access to AMP and/or the Site is provided to Authorized Users only to allow Subscriber to exercise Subscriber's rights under this Agreement. Safety Net Connect and/or its Licensors retain all right, title and interest in and to AMP,

the Site, the Platform, the Site Content and the Safety Net Connect System, including any software and/or databases contained therein, including without limitation, as compilations and expression of distinctive and creative formats. Subscriber agrees to ensure that each authorized copy of any portion of the Site Content will contain the same proprietary notices which appear on AMP or the Site. Safety Net Connect represents and warrants that it has all necessary licenses to provide Subscriber and Authorized Users with the use of AMP, the Site Content and the Safety Net Connect System.

5.2. Subscriber Rights. All right, title and interest in and to the Subscriber Data, as Subscriber's Confidential Information, shall remain exclusively with Subscriber and its licensors, as applicable. Except as set forth in Section 2.5. or Section 9, without the permission of Subscriber, access to the Subscriber Data is provided to Safety Net Connect only to allow Safety Net Connect to fulfill its obligations under this Agreement, including without limitation to diagnose and provide services at Subscriber's request in relation to the Site, the Platform and/or the Site Content.

6. Disclaimer.

Subscriber acknowledges and agrees that any collection and compilation of data entails likelihood of some human and machine errors, omissions, delays, interruptions, and losses, including inadvertent loss of data or damage to media, which may give rise to loss or damage. Accordingly, Subscriber agrees that, except as otherwise provided herein, SAFETY NET CONNECT PROVIDES AMP, THE SITE, THE PLATFORM, THE SITE CONTENT AND THE SAFETY NET CONNECT SYSTEM ON AN "AS IS" AND "WHERE-IS" BASIS. SAFETY NET CONNECT DOES NOT ENDORSE ANY DATA CONTAINED ON AMP OR THE SITE OR WARRANT THAT AMP, THE SITE, THE PLATFORM, THE SITE CONTENT OR THE SAFETY NET CONNECT SYSTEM OR ACCESS THERETO WILL BE ERROR FREE, CURRENT OR UNINTERRUPTED OR THAT ALL ERRORS CAN OR WILL BE CORRECTED. SAFETY NET CONNECT MAKES NO WARRANTIES WITH RESPECT TO THE ACCURACY OF THE INFORMATION CONTAINED ON AMP OR THE SITE OR THE PERFORMANCE OF THE SAFETY NET CONNECT SYSTEM, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND SAFETY NET CONNECT EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

7. Limitations of Liability. INTENTIONALLY OMITTED.

8. Indemnity; Insurance.

8.1. Safety Net Connect Indemnity. In connection with any use of AMP, Safety Net Connect will indemnify, defend, and hold harmless Subscriber 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 the Safety Net Connect Content and the Safety Net Connect System. If a credible claim is made or threatened, including without limitation the filing of a lawsuit against Subscriber, or Subscriber receives a demand or notice claiming actual or potential infringement or misappropriation of any Intellectual Property Rights, Subscriber will use reasonable efforts to notify Safety Net Connect promptly of such lawsuit, claim or election. However, Subscriber's failure to provide or delay in providing such notice will relieve Safety Net Connect of its obligations only if and to the extent that such delay or failure materially prejudices Safety Net Connect's ability to defend such lawsuit or claim. Subscriber will give Safety Net Connect sole control of the defense

(with counsel reasonably acceptable to Subscriber) and settlement of such claim; provided that Safety Net Connect may not settle the claim or suit absent the written consent of Subscriber unless such settlement (a) includes a release of all claims pending against Subscriber, (b) contains no admission of liability or wrongdoing by Subscriber, and (c) imposes no obligations upon Subscriber other than an obligation to stop using the Safety Net Connect Content or the Safety Net Connect System that are the subject of the claim. In the event that Safety Net Connect fails to or elects not to defend Subscriber against any claim for which Subscriber is entitled to indemnity by Safety Net Connect, then Safety Net Connect shall reimburse Subscriber for all reasonable attorneys' fees and expenses within thirty (30) days from date of invoice or debit memo from Subscriber. After thirty (30) days, Subscriber will be entitled to deduct any unpaid invoice or debit memo amount from any amounts owed by Subscriber to Safety Net Connect. This shall not apply to any judgment or settlement amount, which amounts Subscriber shall be entitled to notify, invoice or debit Safety Net Connect's settle the claim or suit. If, in Safety Net Connect's opinion, any Safety Net Connect Content or the Safety Net Connect System becomes, or is likely to becomes, the subject of a claim of infringement of Intellectual Property Rights, Safety Net Connect may, at its option: (i) procure for Subscriber the right to continue using the Safety Net Connect Content or the Safety Net Connect System; (ii) replace or modify the Safety Net Connect Content or the Safety Net Connect System 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 Safety Net Connect, Subscriber shall cease use of the Safety Net Connect Content or the Safety Net Connect System upon written notice from Safety Net Connect, and Safety Net Connect shall provide Subscriber with a pro-rata refund of the unearned fees paid by Subscriber to Safety Net Connect for the Safety Net Connect Content or the Safety Net Connect System.

8.2. Indemnification by Subscriber. INTENTIONALLY OMITTED. 8.3. Insurance. Without in anyway affecting the indemnity herein provided and in addition thereto, Safety Net Connect shall secure and maintain throughout the contract term Cyber liability Insurance *w*ith limits of no less than $1,000,000 for each occurrence or event with an annual aggregate of $2,000,000 covering claims involving violation, 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 Subscriber entities and cover breach response cost as well as regulatory fines and penalties. The policy shall contain endorsements naming Subscriber and its officers, employees, agents and volunteers as additional 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 Subscriber to vicarious liability but shall allow coverage for the Subscriber to the full extent provided by the policy. Safety Net Connect shall require its carriers to waive all rights of subrogation against the Subscriber, its officers, employees, agents, volunteers, contractors and subcontractors. Safety Net Connect hereby waives all rights of subrogation against the Subscriber. All policies required herein are to be primary and non-contributory with any insurance or self-insurance programs carried or administered by the Subscriber. Safety Net Connect 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 Safety Net Connect and the Subscriber or between the Subscriber and any other insured or additional insured under the policy. Safety Net Connect shall furnish Certificates of Insurance to the Subscriber evidencing the insurance coverage, including endorsements, as required, 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 Subscriber, and Safety Net Connect shall maintain such insurance from the time Safety Net Connect commences performance of services hereunder until the completion of such services. Within fifteen

(15) days of the commencement of this contract, Safety Net Connect 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. Unless otherwise approved by Subscriber, 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". 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 Subscriber has the right but not the obligation or duty to cancel the contract, without incurring any cancellation or termination charges, or obtain insurance if it deems necessary and any premiums paid by the Subscriber will be promptly reimbursed by Safety Net Connect or Subscriber payments to Safety Net Connect will be reduced to pay for Subscriber purchased insurance.

9. Confidential Information.

9.1. Definition of Confidential Information. For the purposes of this Agreement, "Confidential Information" means any and all (i) technical and non-technical information including patent, trade secret and proprietary information, techniques, sketches, drawings, models, inventions, know-how, processes, apparatus, equipment and algorithms related to AMP, the Site, the Platform, Site Content, and related documentation, (ii) information relating to costs, prices and names, finances, marketing plans, business opportunities, personnel, research, development or know-how; and (iii) all non-public Subscriber Data; and (iv) information designated by either party as confidential in writing or, if disclosed orally, reduced to writing within thirty (30) days. Notwithstanding the foregoing, "Confidential Information" shall not include information that: (1) is or becomes generally known or available by publication, commercial use or otherwise through no fault of the disclosing party; (2) is known and has been reduced to tangible form by the disclosing party at the time of disclosure and is not subject to restriction; (3) is independently developed or learned by either party; (4) is lawfully obtained from a third party who has the right to make such disclosure; (5) is released for publication in writing; (6) or is required to be disclosed under government public records and open meetings laws.

9.2. Nondisclosure and Nonuse Obligation. Each party agrees that it will not and will ensure that its employees, agents and contractors will not make use of, disseminate, or in any way disclose any Confidential Information of the other party to any person, firm or business, except for any purpose the disclosing party may hereafter authorize in writing. Each party agrees that it will treat all Confidential Information with the same degree of care as it accords to its own Confidential Information, and each party represents that it exercises reasonable care to protect its own Confidential Information.

9.3. Business Associate Obligations. Safety Net Connect acknowledges that it is a "business associate" of Subscriber as that term is defined in the federal Health Insurance Portability and Accountability Act (HIPAA) and its associated regulations. The parties agree that the provisions of the attached "Business Associate Agreement" apply to the use by and disclosure of information through this software solution and that in the event of any conflict between the provisions of the Business Associate Agreement and this agreement the Business Associate Agreement provision will prevail.

10. Term and Termination.

10.1. Term. This Agreement shall be effective as of March 1, 2020 ("Effective Date") and shall continue in effect February 28, 2025 ("Initial Term") unless earlier terminated in accordance with the provisions of the MSA.

10.2. Termination for Cause. Safety Net Connect or Subscriber may terminate this Agreement upon thirty (30) days' written notice of a material breach of this Agreement if such breach is not cured within such thirty (30) day period.

10.3. Obligations of the Parties Upon Expiration or Termination. Upon the expiration or termination of the Agreement, (i) each party will return to the other party any Confidential Information of the other party; (ii) Subscriber will disable any hypertext link between the Subscriber site on the World Wide Web to AMP and/or the Site; and (iii) Subscriber and each Authorized User will no longer be provided access to AMP or the Site and shall immediately return to Safety Net Connect all copies of the Site Content and the related documentation in its possession or control. In addition, on or before the effective date of termination, Safety Net Connect will provide Subscriber with a copy of the most recent back up of the Subscriber Data in a format reasonable agreed by the parties, and will make commercially reasonable efforts to assist Subscriber in the transition of such Subscriber Data as reasonably requested by Subscriber. Upon request, either will, within ten (10) days of termination, certify in writing its compliance with this Paragraph to the other party.

11. General Conditions.

11.1. Governing Law. Any disputes under this Agreement shall be resolved under California law without reference to conflict of laws principles.

11.2. Publicity. INTENTIONALLY OMITTED.

11.3. Waiver. No waiver of any right under this Agreement shall be deemed effective unless contained in writing signed by a duly authorized representative of the party against which the waiver is sought to be enforced, and no waiver of any past or present right arising from any breach or failure to perform shall be deemed to be a waiver of any future right arising under this Agreement.

11.4. Severability. If any provision in this Agreement is invalid or unenforceable, that provision shall be construed, limited, modified or, if necessary, severed, to the extent necessary, to eliminate its invalidity or unenforceability, and the other provisions of this Agreement shall remain in full force and effect.

11.5. Assignment. This Agreement is not assignable by either party without the prior written consent of the other party, which consent shall not be unreasonably withheld. Any attempt at assignment, including by means of merger, acquisition, operation of law or otherwise, without such consent shall be null and void and of no force and effect.

11.6. Compliance with Laws. Each party agrees to comply with all applicable laws and regulations with respect to its activities hereunder, including but not limited to any export and securities laws and regulations of the United States.

11.7. Force Majeure. INTENTIONALLY OMITTED.

11.8. Notices. Any notice required or permitted to be sent under this Agreement shall be delivered by hand, by overnight courier or by certified mail, return receipt requested, to the address of the parties

set forth in this Agreement or to such other address of the parties designated in writing in accordance with this subsection and is effective upon receipt.

11.9. Entire Agreement. This Agreement sets forth the entire understanding and agreement between Subscriber and Safety Net Connect and supersedes all prior or contemporaneous proposals or communications, oral or written, between the parties relating to the subject matter of the Agreement. No modification of the Agreement shall be binding unless it is in writing and is signed by authorized representatives of both parties.

11.10. Survival. The following provisions of this Agreement shall survive any termination or expiration of this Agreement: Section 5 ("Proprietary Rights"), Section 6 ("Disclaimer") Section 7 ("Limitations of Liability"), Section 8 ("Recourse; Indemnities"), Section 9 ("Confidential Information"), Section 10 ("Term and Termination"), and Section 11 ("General Conditions").

IN WITNESS WHEREOF, the authorized representatives of the parties have executed this Agreement as of the date last signed below.

IN WITNESS WHEREOF, the authorized representatives of the parties have executed this Agreement as of the date last signed below.

SAFETY NET CONNECT:

COUNTY OF SAN BERNARDINO on behalf of ARROWHEAD REGIONAL MEDICAL CENTER

By: _____

By: _____

Authorized Signature

Authorized Signature

Name: Chris Cruttenden_____

Name: Curt Hagman

Title: President_____

Title: Chairman, Board of Supervisors

Date: _____

ATTACHMENT H

Data Storage, Segregation and Access Controls Addendum

Safety Net Connect ("SNC") represents and warrants that its eConsult application will be operated and maintained throughout the term of the Professional Services Agreement with the data storage, segregation and access controls described in this Agreement. SNC further warrants that any additional or different data storage, segregation or access control measures it wishes to employ with regard to eConsult will be described and agreed to, prior to deployment, in a written addendum to this Agreement signed by both parties.

SNC runs and manages their enterprise business applications from a collocated hosting environment. This fault-tolerant, clustered environment resides on company owned hardware and storage located entirely in the United States at the AT&T Internet Data Centers (primary site Irvine, CA; secondary site Lisle, IL). Our servers are deployed in an isolated environment within locked cabinets and are protected behind multiple security firewalls. AT&Ts state of the art datacenters provide colocation services, which include the assignment of IP space, network connectivity, 24-hour advanced security services, and delivery of power. Only approved system administrators have access to our locked cabinets within the AT&T data centers. The data centers have full 24 hour guarded access that include biometrics, man-traps, and access cards.

The ePHI available through the MCEI eConsult system is stored in SNC Enterprise Database Servers. SNC deploys a multi-tenant database architecture. The MCEI ePHI is stored within self-contained database schemas, logically in the form of tablespaces and physically in the form of data files. Access to these schemas is strictly limited to the MCEI applications and appropriately permissioned system administrators. No other methods of accessing the ePHI are permitted. In addition, uploaded data stored in the system is encrypted and decrypted using an MCEI specific PKI key pair.

Within the MCEI eConsult instance, we employ role-based access to the data. This ensures that only properly credentialed users can access any of the data. We segment the data within the instance by what we call NETWORKS. Only logged in users associated with organizations tied to a specific NETWORK can access any of that NETWORK's data. The data access rules can be customized based on the business rules required by the client(s). Access to each NETWORK's contributed data is denied by default. A user must be granted explicit permissions access to the data. Each NETWORK will have the ability to designate administrators who manage the user permissions for their NETWORK.

Data segregated by Network:

Data Category	Access Rules
Patient Data	Only users permissioned to the NETWORK will have access to that network's patients. Access includes: • Ability to search for patients within the NETWORK to support the submission of eConsults

	• Viewing Patient Demographic information Standard Patient Demographic Fields: • Name • Date of Birth • Gender • Member ID / Insurance ID • Mother's Maiden Name • Spoken/Preferred Language (TBD: Final fields still under review with each respective group) The only data users will see are specific demographic fields used to positively identify the patient and submit an eConsult. No clinical information is visible in the patient search (See Consult Data category for specified data fields).
Consult Data	By default only users permissioned to the submitting site (PCP/Staff), reviewing site (Specialist Reviewer) or the referred site (Specialty Clinic for Face to Face Visits) can view eConsults. Only those explicitly involved with the Consult are allowed to view the eConsult data. Consults will contain: • Diagnosis Code • Requested Procedure Code • Clinical Question • Clarifying Question Answers • Uploaded Documents • eConsult Dialog between PCP and Specialist Reviewer The "Network Admin" can view and search consults across the entire NETWORK(s) that they are permissioned to. Note: To support integration with IEHP's Authorization System (MedHok) the eConsult platform will need to send Patient and Consult Data for Authorization purposes.

Security measures and Breach Policies

SNC deploys multiple firewalls protecting stored ePHI are equipped with an intelligent intrusion detection system (IDS) and enforce security between networks by controlling and restricting traffic flows. The IDS immediately alert system administrators when an intrusion attempt has occurred and prevents future accesses from the source of the attempted intrusion.

Other countermeasures maintained by SNC to control inappropriate ePHI access include:
• Configure firewall to alert immediately when IDS detect a significant event

- Enforce deployment of latest security patches for OS, database, and Web server
- Enforce security code review
- Enforce data access via stored procedures or formal parameters content validation
- Implement validation of input fields in web pages
- Review secured passwords and role-based mechanism for web users
- Review monitoring mechanism for back-end processing (system health)
- Continue to limit access of clients and employees to system resources
- Enforce quality passwords policy for protecting each of the machines on the network
- Database login accounts are given the minimal rights that are necessary for their functionality

SNC employs a centralized logging server across all SNC systems. The central logging server provides searches that are used to detect errors throughout the environment (unix servers, web servers, database servers, firewalls, switches, etc). This allows SNC to audit and monitor accounts with login privileges, as well as user activity such as failed login attempts and successful logins.

The SNC proprietary access audit and reporting module tracks individual data level access to ePHI (and other tagged data) in the MCEI database. It allows appropriately permissioned administrators to easily track user access to ePHI.

SNC maintains a comprehensive Information Security Policy that defines the team members, roles and responsibilities required to respond to various types of incidents (including potential breaches, emergencies and disasters). SNC's Information Security Policy includes system and application logging requirements as well as access audits. This policy outlines rules for accessing, storing, handling, protecting, distributing and disposing of data. The Information Security Policy contains measures that:

- Ensure that the minimum amount of secure data is stored on the system at any time
- Has a security officer who assures the personal integrity of employees
- Ensure that only the minimum necessary ePHI is displayed to the end users in accordance with HIPAA Privacy Rule requirements
- Enforce employees' liability and discipline for unauthorized use or disclosure of ePHI

Encrypted backups of the ePHI data are performed nightly to disk and then to LTO Tape Jukeboxes. Full backup tapes are transported to a secure off-site location for long term storage. Additionally, SNC employs replication technology to support local and off-site data replication. This technology provides rapid data restores, multiple restore points, and reduced recovery point objectives.

The operating environment at the off-site location closely matches the primary production systems. In the event of a disaster that renders the primary systems inoperable, system operations will be directed to the SNC offsite location.

SNC has earned its HIPAA HITEC Certification and its Service Organization Control (SOC) 2 Certification through NetChemistry, Inc.. The SOC 2 report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and

privacy of a system, as opposed to SOC 1/SSAE 16 which is focused on the financial reporting controls. Additionally, SNC complies with **Experian's EI3PA** assessment criteria.