

i2i Systems, Inc.
Data Sharing Agreement

This Data Sharing Agreement (“**DSA**”), effective as of _____ (the “**Effective Date**”) is by and between i2i Systems, Inc., having its principal place of business at 377 Riverside Drive, Suite 300, Franklin, TN 37064 (“**i2i**”) and Tulare County Health & Human Services Agency, having its principal place of business at 5957 South Mooney Blvd., Visalia, CA 93277 (“**Customer**”), each referred to herein as a “**Party**” and collectively as the “**Parties**”.

Recitals

WHEREAS, i2i provides a proprietary population health management interface that connects to EMRs and PMs to extract and aggregate clinical and financial data, identify at-risk populations, assign personalized actionable care pathways, and engage patients in evidence-based interventions across specific care teams;

WHEREAS, i2i has contractual relationships, including, but not limited to, agreements regarding the secure transfer and maintenance of privacy, security, and confidentiality of patient and other health information, with certain groups that finance, fund, reimburse, and/or support the cost of health services of Customer (the “**Payers or Sponsors**”);

WHEREAS, Customer and certain health care providers affiliated with Customer (the “**Providers**”), provide health services to patients (the “**Customer Patients**”);

WHEREAS, Customer, Providers, and Customer Patients have a contractual relationship with Payers or Sponsors, under which Payers or Sponsors are authorized to receive Customer Patient data; and

WHEREAS, Customer desires i2i to share Customer Patient data with the Payers or Sponsors.

Agreement

NOW, THEREFORE, in consideration of the mutual covenants, terms and conditions set forth above and herein, and for other good and valuable consideration, including, but not limited to, benefit from the mutual relationship with the Payers or Sponsors, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. **Service.** For the purposes of this DSA, the “**Service**” shall mean i2i’s interface with Customer’s Electronic Medical Record (EMR) and other ancillary systems to extract relevant patient data. i2i will then cross-reference Customer Patient data and share the Customer Patient data. Customer acknowledges and agrees that full cooperation with i2i is necessary to accomplish the Service, including, but not limited to, coordinating integration with Customer’s technology team, as reasonably required. Once extraction and sharing is complete, i2i will provide a report to Customer identifying the affiliated Provider and detailing the Customer Patient data that was shared with the Payers or Sponsors.
2. **Grant of Right to Use the Service.** i2i grants to Customer a non-exclusive, personal, nontransferable, limited license to use any interface furnished by i2i for the Service, to assist in establishing the interface with Customer’s EMR system.
3. **Term.** The term of this DSA shall begin on the Effective Date and shall end upon termination by either party pursuant to the terms of this section. Either Party may terminate this DSA by providing the other Party sixty (60) days’ prior written notice. However, Customer understands that due to the nature of the Services, i2i must notify the Payers or Sponsors of a termination of this DSA and customer

acknowledges and agrees such termination may affect Customer's contractual relationship with the Payers or Sponsors and may be considered a breach thereof.

4. Business Associate Agreement. The Parties agree that this DSA involves the transfer of patient health information (PHI) and electronic PHI, as defined and governed in the Health Insurance Portability and Accountability Act of 1996, the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), and their implementing regulations set forth at 45 C.F.R. Parts 160, 162, and 164, as amended. Therefore, the parties agree to simultaneously with this DSA enter into a Business Associate Agreement ("BAA"), the terms of which are hereby incorporated by reference. A form BAA is attached hereto as **Exhibit B**. In the event of any conflict between the terms of the main body of this DSA and the terms of the BAA, the terms of the BAA shall prevail for purposes of matters set forth in the BAA.

5. Customer Permissions. Customer acknowledges and agrees that the Services involve the sharing of Customer Patient data with certain Payers or Sponsors. Customer acknowledges and agrees that the Service is being conducted at the request and direction of such certain Payers or Sponsors. Customer hereby authorizes i2i to utilize the service to transfer Customer patient data to the Payers or Sponsors included in **Exhibit A**, attached hereto. i2i may update the list of Payers or Sponsors in **Exhibit A** from time to time, at its discretion, which update will be deemed an amendment upon reasonable notice to Customer.

6. Payer or Sponsor Relationship. i2i makes no representations or warranties regarding the terms of any agreement with the Payers or Sponsors that Customer or the Providers are parties to. Furthermore, Customer acknowledges and agrees that Customer should rely on its own independent legal advisors for any questions or concerns regarding any such agreement with the Payers or Sponsors.

7. Third-Party Services. The Service may include certain third-party software and services, which may require that Customer enter into separate subscription or licensing agreements with third-party vendors. i2i may also make available optional services provided by third parties. Customer agrees to comply with, and upon request, to execute, such agreements as may be required for the use of such software or services, and to comply with the terms of any license or other agreement relating to third-party products included in the Service or made to Customer through the Service. Customer's use of the Service or of such third-party products or services will constitute Customer's agreement to be bound by the terms of all licensing, subscription and similar agreements relating to such use.

8. Verification. Customer acknowledges and agrees that the Service is subject to verification by i2i of Customer credentials as a health care practitioner or other health care entity with a declared relationship pursuant to the applicable Privacy Rules and to Customer's ongoing qualification as such. Customer agrees that i2i may use and disclose personal information for such purposes, including (without limitation) making inquiry of third parties concerning identity and professional, practice, or other related credentials. Customer agrees to hold i2i harmless from any claim or liability arising from the request for or disclosure of such information. Customer agrees that i2i may terminate use of the Service at any time if i2i is unable at any time to determine or verify qualifications or credentials of Customer.

9. Prohibited Uses. Customer agrees that it will not access or use the Services to (a) reproduce, publish, or distribute content in connection with the Service that infringes i2i or any third-party's trademark, copyright, patent, trade secret, publicity, privacy, or other personal or proprietary right; (b) abuse or misuse the Services, including gaining or attempting to gain unauthorized access, or altering or destroying information except in accordance with this DSA; or (c) Customer will never use the Service to advise, diagnose, or otherwise treat patients.

10. Compliance with Laws. The Parties agree to comply with all applicable laws, including, but not limited to, laws relating to maintenance of privacy, security, and confidentiality of patient and other health

information and laws relating to the prohibition on the use of telecommunications facilities to transmit illegal, obscene, threatening, libelous, harassing, or offensive messages, or otherwise unlawful material.

11. Access to Data. Customer acknowledges and agrees that i2i will access patient data held by Customer in order to facilitate coordination of care and other health care operations pursuant to the restrictions contained in applicable law, including but not limited to, 45 CFR §164.506. Customer specifically agrees that such access, retention of data, and release of data by i2i, subject to the restrictions of applicable law, shall not constitute a breach of this DSA.

12. Notices. Any notice, request, or other communication to be given in writing in connection with this Agreement shall be deemed given as of the day they are received by messenger or overnight courier service or three (3) business days after being sent by certified, first class, postage pre-paid mail, to the following addresses, or to such other address as the party to receive the notice or request so designates by written notice to the other:

i2i: i2i Population Health
377 Riverside Drive, Suite 300
Franklin, TN 37064
Attn: President

With Copy to: Sarah Casey
100 South Ashley Drive, Suite 375
Tampa, FL 33602
Fax: (813) 434-2278

Customer: _____

Attn: _____

13. Insurance. Prior to approval of this agreement by the COUNTY, i2i Systems, Inc. shall file with the Clerk of the Board of Supervisors evidence of required insurance as set forth in Exhibit C attached, which outlines the minimum scope, specifications and limits of insurance required under this contract. Additional insured endorsements required as outlined in Exhibit C shall not be used to reduce limits available to County as an additional insured from i2i Systems, Inc. full policy limits. Insurance policies shall not be used to limit liability or to limit the indemnification provisions and requirements of this contract or act in any way to reduce the policy coverage and limits available from the insurer (s). Failure to maintain or renew coverage, or to provide evidence of renewal, may be considered a material breach of this Agreement.

14. Entire Agreement. The recitals included above are hereby incorporated into this DSA and this DSA, along with the exhibit attached hereto, contains the entire agreement of the Parties and supersedes all other agreements of the Parties, whether written or oral, with respect to the subject matter contained herein.

[Signature Page Follows]

IN WITNESS WHEREOF, the duly authorized representatives of the Parties have executed this DSA as of the Effective Date.

Signatures

Tulare County Health Services

Signed: _____

Name: _____

Title: _____

Date: _____

i2i Systems, Inc.

Signed:  _____

Name: Justin L. Neece

Title: President and Chief Executive Officer

Date: 08/16/2019

APPROVE AS TO FORM:

COUNTY COUNSEL
BY  _____
DEPUTY

8/23/19

20196661

Exhibit A

List of Payers or Sponsors

Payer or Sponsor Name and Address
1. Health Net, Inc.
2.
3.
4.
5.
6.

Exhibit B

[Business Associate Agreement]

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“BAA”) supplements and is made a part of the Data Sharing Agreement between **i2i Systems, Inc.**, having its principal place of business at 377 Riverside Drive, Suite 300, Franklin, TN 37064 (“**Business Associate**”), and **Tulare County Health & Human Services Agency**, having its principal place of business at 5957 South Mooney Blvd., Visalia, CA 93277 (“**Covered Entity**”). Either party may be referred to individually as the “**Party**” or collectively as the “**Parties**”.

Background

In providing the services under the Data Sharing Agreement (“DSA”) to which this BAA is attached as Exhibit B, Covered Entity and Business Associate enter into this BAA to comply with the requirements of the implementing regulations at 45 Code of Federal Regulations (“C.F.R.”) Parts 160-64 for the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), and the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the “HITECH Act”), that are applicable to business associates, along with any guidance or regulations issued by Department of Health and Human Services (“HHS”). Covered Entity and Business Associate agree to incorporate into this BAA any regulations issued with respect to the HITECH Act that relate to the obligations of business associates. Business Associate recognizes and agrees that it is obligated by law to meet the applicable provisions of the HITECH Act.

1. Definitions

- 1.1 Terms used, but not otherwise defined, in this BAA shall have the same meaning as those terms in 45 CFR §§ 160.103, 164.304, 164.504 and 164.501.
- 1.2 “Designated Record Set” shall have the meaning set out in its definition at 45 CFR § 164.501.
- 1.3 “Electronic Protected Health Information” or “EPHI” means Protected Health Information (PHI) that is transmitted by or maintained in electronic media as set out in 45 CFR § 160.103.
- 1.4 “Health Care Operations” shall have the meaning set out in its definition at 45 CFR § 164.501.
- 1.5 “Individual” shall have the same meaning as the term “individual” in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.
- 1.6 “Limited Data Set” means protected health information that excludes the direct identifiers of the individual or of relatives, employers, or household members of the individual delineated under 45 CFR § 164.514(e)(2).

- 1.7 “Privacy Officer” shall have the meaning as set out in its definition at 45 CFR § 164.530(a)(1). The Privacy officer is the official designated by a Covered Entity or Business Associate to be responsible for compliance with HIPAA regulations.
- 1.8 “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, subparts A, and E.
- 1.9 “Protected Health Information” or “PHI” shall have the same meaning as the term “protected health information” in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity. PHI includes information in any format, including, but not limited to, electronic or paper.
- 1.10 “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR § 164.501.
- 1.11 “Security Incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as provided in 45 C.F.R. § 164.304.
- 1.12 “Security Event” means an immediately reportable subset of security incidents which incident would include:
- a) a suspected penetration of Business Associate’s information system of which the Business Associate becomes aware, but for which it is not able to verify within forty-eight (48) hours (of the time the Business Associate became aware of the suspected incident) that PHI or other confidential data was not accessed, stolen, used, disclosed, modified, or destroyed;
 - b) any indication, evidence, or other security documentation that the Business Associate’s network resources, including, but not limited to, software, network routers, firewalls, database and application servers, intrusion detection systems or other security appliances, may have been damaged, modified, taken over by proxy, or otherwise compromised, for which Business Associate cannot refute the indication within forty-eight (48) hours of the time the Business Associate became aware of such indication; and/or
 - c) the unauthorized acquisition, including, but not limited to, access to or use, disclosure, modification or destruction, of unencrypted PHI or other confidential information of the Covered Entity by an employee or authorized user of Business Associate’s system(s), which materially compromises the security, confidentiality, or integrity of PHI or other confidential information of the Covered Entity.

If data acquired (including, but not limited to, access to or use, disclosure, modification or destruction of such data) is in encrypted format but the decryption key which would allow the decoding of the data is also taken, the parties shall treat the acquisition as a breach for purposes of determining appropriate response.

- 1.13 “Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information” at 45 CFR Parts 160 and 164, Subparts A and C, and any other applicable provision of HIPAA, and any amendments thereto, including HITECH.

- 1.14 “Unsecured PHI” shall mean PHI or ePHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued pursuant to § 13402 of the HITECH Act, as provided in 45 C.F.R. § 164.40.2.

2. Permitted Uses and Disclosures of Business Associate

- 2.1 Operations on Behalf of Covered Entity. Pursuant to the terms herein or any written agreement with Covered Entity, Business Associate is permitted to use and disclose PHI that it creates or receives on Covered Entity’s behalf or receives from Covered Entity or another business associate of Covered Entity (collectively, “Covered Entity’s Protected Health Information”).
- 2.2 Business Associate’s Operations. Except as otherwise limited in this BAA, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 42 C.F.R. § 164.504(e)(2)(i)(B). Business Associate may de-identify PHI received from Covered Entity and use such de-identified data, consistent with the Privacy Rule’s standards for de-identification. 45 C.F.R. § 164.514. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 42 C.F.R. § 164.502(j)(1). Business Associate may use PHI for its proper management and administration or to carry out Business Associate’s legal responsibilities.

3. Obligations of Business Associate

- 3.1 Compliance with the Privacy Rule. Business Associate agrees to use appropriate safeguards to prevent disclosure of the PHI other than as provided for by this BAA, and to implement administrative, physical, and technical safeguards as required by 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316 in order to protect the confidentiality, integrity, and availability of PHI that the Business Associate receives, creates, maintains or transmits to the same extent as if the Business Associate were a Covered Entity. The Business Associate shall undertake such actions in a manner that is consistent with any guidance issued by the Secretary pursuant to the HITECH Act.
- 3.2 Business Associate Contracts. Business Associate shall require any agent, including a subcontractor, to whom it provides PHI received from, maintained, created or received by Business Associate on behalf of Covered Entity, or that carries out any duties for the Business Associate involving the use, custody, disclosure, creation of, or access to PHI or other confidential information, to agree, by written contract with Business Associate, to the same restrictions and conditions that apply through this BAA to Business Associate with respect to such information.
- 3.3 Mitigation of Harmful Effect of Violations. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this BAA.
- 3.4 Privacy Obligation Breach and Security Incidents.
- 3.4.1 Privacy Breach. Business Associate will report to Covered Entity any use or disclosure of Covered Entity’s Protected Health Information not permitted by this BAA or in writing by Covered Entity. In addition, Business Associate will report, following discovery and without unreasonable delay, but in no event later than

fifteen (15) calendar days following discovery, any "Breach" of "Unsecured Protected Health Information" as these terms are defined by the HITECH Act and any implementing regulations. Business Associate shall notify the Covered Entity of any Security Incident which would constitute a Security Event as defined by this BAA in a preliminary report within fifteen (15) calendar days and with a full report of the incident not less than thirty (30) calendar days after it became aware of the incident. Business Associate shall cooperate with Covered Entity in investigating the Breach and in meeting the Covered Entity's obligations under the HITECH Act and any other security breach notification laws. In the event of a breach, Business Associate and Covered Entity will work together to comply with any required regulatory filings.

- 3.4.2 Report. Any such report shall include the identification (if known) of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Business Associate will make the report to Covered Entity not more than fifteen (15) calendar days after Business Associate learns of such non-permitted use or disclosure. Business Associate's initial report will include, to the extent such information is available, the Individual's affected, the PHI affected, the nature of the non-permitted access, use or disclosure, and the steps Business Associate took to secure the PHI.
- 3.4.3 Security Incidents. Business Associate will report to Covered Entity any attempted or successful (A) unauthorized access, use, disclosure, modification, or destruction of Covered Entity's Electronic Protected Health Information or (B) interference with Business Associate's system operations in Business Associate's information systems, of which Business Associate becomes aware. Business Associate will make this report upon Covered Entity's request, except if any such security incident resulted in a disclosure of Covered Entity's Protected Health Information not permitted by this BAA, Business Associate will make the report in accordance with Section 2.6.1.
- 3.5 Audit Reporting. Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to Covered Entity, or at the request of Covered Entity, to the Secretary, for purposes of determining Covered Entity's or Business Associate's compliance with HIPAA.
- 3.6 Access of Individual to PHI and other Requests to Business Associate. If Business Associate receives PHI from Covered Entity in a Designated Record Set, Business Associate agrees to provide access to PHI in a Designated Record Set to Covered Entity in order to meet its requirements under 45 CFR § 164.524. If Business Associate receives a request for PHI in the possession of the Covered Entity, or receives a request to exercise other individual rights as set forth in the Privacy Rule, Business Associate shall promptly forward the request to Covered Entity within five (5) business days. Business Associate shall then assist Covered Entity as necessary in responding to the request in a timely manner. If Business Associate provides copies of PHI to the individual, it may charge a reasonable fee for the copies as the regulations shall permit.
- 3.7 Requests to Covered Entity for Access to PHI. The Covered Entity shall forward to the Business Associate within five (5) business days any Individual's request for access to or

a copy of their PHI that shall require Business Associate's participation, after which the Business Associate shall provide access to or deliver such information.

- 3.8 Individuals' Request to Amend PHI. If Business Associate receives PHI from Covered Entity in a Designated Record Set, Business Associate agrees to make any amendments to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR § 164.526, regarding an Individual's request to amend PHI. The Business Associate shall make the amendment promptly in the time and manner designated by Covered Entity, but shall have thirty (30) calendar days' notice from Covered Entity to complete the amendment to the Individual's PHI and to notify the Covered Entity upon completion.
- 3.9 Recording of Designated Disclosures of PHI. Business Associate agrees to document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.
- 3.10 Accounting for Disclosures of PHI. The Business Associate agrees to provide to Covered Entity or to an Individual, in time and manner designated by Covered Entity, information collected in accordance with this BAA, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. The Covered Entity shall forward the Individual's request requiring the participation of the Business Associate to the Business Associate within five (5) business days, after which the Business Associate shall provide such information.
- 3.11 Minimum Necessary. Business Associate agrees it must limit any use, disclosure, or request for use or disclosure of PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the requirements of the Privacy Rule.
- 3.12 Security and Privacy Compliance Review upon Request. Business Associate agrees to make its internal practices, books and records, including policies, procedures, and PHI, relating to the use and disclosure of PHI received from, created by or received by Business Associate on behalf of Covered Entity available to the Covered Entity or to the Secretary of the United States Department of Health in Human Services or the Secretary's designee, in a time and manner designated by the requester, for purposes of determining Covered Entity's or Business Associate's compliance with the Security & Privacy Rules.
- 3.13 Cooperation in Security & Privacy Compliance. Business Associate agrees to fully cooperate in good faith and to assist Covered Entity in complying with the requirements of the Security & Privacy Rules.
- 3.14 Contact for Security Event Notice. Notification for the purposes of notification shall be in writing made by certified mail or overnight parcel, with supplemental notification by facsimile, email, or telephone as soon as practicable, to the respective Party at the address first included above.

4. Obligations of Covered Entity

- 4.1 Notice of Privacy Practices. Covered Entity shall provide Business Associate with the notice of Privacy Practices produced by Covered Entity or provided to Covered Entity as

a result of Covered Entity's obligations with other organizations in accordance with 45 CFR § 164.520, as well as any changes to such notice.

- 4.2 Notice of Changes in Individual's Access or PHI. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses.
- 4.3 Notice of Restriction in Individual's Access or PHI. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use of PHI.
- 4.4 Restriction on Requests. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rules if done by Covered Entity.

5. Term and Termination

- 5.1 Term. This BAA shall be effective as of the date on which it has been signed by both parties and shall terminate when while any PHI which has been provided, regardless of form, pursuant to the DSA is still in possession of Business Associate.
- 5.2 Termination for Cause. This BAA authorizes Covered Entity, and Business Associate acknowledges and agrees Covered Entity shall have the right, to immediately terminate this BAA in the event Business Associate fails to comply with, or violates a material provision of, this BAA or any provision of the Privacy or Security Rules.
 - 5.2.1 Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:
 - a) Provide notice of breach and an opportunity for Business Associate to reasonably and promptly cure the breach or end the violation, and terminate this BAA if Business Associate does not cure the breach or end the violation within the reasonable time specified by Covered Entity; or
 - b) Immediately terminate this BAA if Business Associate has breached a material term of this BAA and cure is not possible; or
 - c) If termination, cure, or end of violation is not feasible, Covered Entity shall report the violation to the Secretary.
- 5.3 Effect of Termination. In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make the return or destruction of such information infeasible. Upon such notification, Business Associate shall extend the protections of this BAA to such PHI, and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

6. MISCELLANEOUS

- 6.1 **Regulatory Reference.** A reference in this BAA to a section in the Privacy or Security Rule means the section as in effect or as amended.
- 6.2 **Modification and Amendment.** This BAA may be modified only by express written amendment executed by the Parties. The Parties agree to take such action to amend this BAA from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act, Public Law 104-191.
- 6.3 **State and Federal Compliance.** The Business Associate shall comply with all applicable State and Federal laws and regulations in the performance of this BAA.
- 6.4 **Interpretation.** Any ambiguity in this BAA shall be resolved in favor of a meaning that permits Covered Entity and the Business Associate to comply with the Privacy and Security Rules.
- 6.5 **Headings.** Paragraph Headings, as used in this BAA, are for the convenience of the Parties and shall have no legal meaning in the interpretation of the BAA.
- 6.6 **Notice.** All notices, requests, demands, and other communications required or permitted to be given under this BAA shall be in writing, and shall be effective upon receipt. Such notice may be made by personal delivery, by facsimile or electronic mail with return facsimile or electronic mail acknowledging receipt, by overnight delivery service with proof of delivery, or by certified or registered United States mail, return receipt requested. All such communications shall be sent to the respective Party at the address first included in the DSA.
- 6.7 **Strict Compliance.** No failure by any Party to insist upon strict compliance with any term or provision of this BAA, to exercise any option, to enforce any right, or to seek any remedy upon any default of any other Party shall affect, or constitute a waiver of, any Party's right to insist upon such strict compliance, exercise that option, enforce that right, or seek that remedy with respect to that default or any prior, contemporaneous, or subsequent default. No custom or practice of the Parties at variance with any provision of this BAA shall affect, or constitute a waiver of, any Party's right to demand strict compliance with all provisions of this BAA.
- 6.8 **Severability.** Any provision of this BAA that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.
- 6.9 **Governing Law.** This BAA shall be governed by and construed in accordance with the laws of the State of Tennessee except to the extent that said law has been pre-empted by HIPAA or HITECH.
- 6.10 **Conflicts.** The terms and conditions of this BAA will override and control any conflicting term or condition of any other agreement between the Parties. All nonconflicting terms and conditions of other agreements between the Parties remain in full force and effect.

END OF CONTRACT TERMS

Covered Entity

Tulare County Health Services

Signed: _____

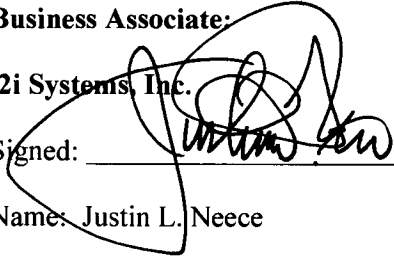
Name: _____

Title: _____

Date: _____

Business Associate:

i2i Systems, Inc.

Signed: _____ 

Name: Justin L. Neece

Title: President and Chief Executive Officer

Date: 08/16/2019

EXHIBIT C

IT PROFESSIONAL SERVICES CONTRACTS **INSURANCE REQUIREMENTS**

CONSULTANT shall provide and maintain insurance for the duration of this Agreement against claims for injuries to persons and damage to property which may arise from, or in connection with, performance under the Agreement by the CONSULTANT, his agents, representatives, employees and subcontractors, if applicable.

A. Minimum Scope & Limits of Insurance

1. Coverage at least as broad as Commercial General Liability, insurance Services Office Commercial General Liability coverage occurrence form GC 00 01, with limits no less than \$1,000,000 per occurrence including products and completed operations, property damage, bodily injury and personal & advertising injury. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this project/location (ISO CG 25 03 or 25 04) or the general aggregate limit shall be twice the required occurrence limit.
2. Insurance Services Office Form Number CA 00 01 covering Automobile Liability, (any auto) of \$1,000,000 per occurrence. If an annual aggregate applies it must be no less than \$2,000,000.
3. Workers' Compensation insurance as required by the State of California, with Statutory Limits, and Employer's Liability Insurance with limit of no less than \$1,000,000 per accident for bodily injury or disease.
4. Technology Professional Liability (Errors and Omissions) Insurance appropriate to the CONSULTANT's profession, with limits no less than \$1,000,000 per occurrence or claim, \$2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Consultant in this agreement and shall include, but not limited to, claims involving infringement of intellectual property, infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties, credit monitoring expenses.

B. Specific Provisions of the Certificate

1. If the required insurance is written on a claims made form, the retroactive date must be before the date of the contract or the beginning of the contract work and must be maintained and evidence of insurance must be provided for at least three (3) years after completion of the contract work.
2. CONSULTANT must submit endorsements to the General Liability reflecting the following provisions:
 - a. *The COUNTY, its officers, agents, officials, employees and volunteers are to be covered as additional insureds as respects: liability arising out of work or operations performed by or on behalf of the CONSULTANT; or automobiles owned, leased, hired or borrowed by the CONSULTANT.*
 - b. *For any claims related to this project, the CONSULTANT's insurance coverage shall be primary insurance as respects the COUNTY, its officers, agents, officials, employees and volunteers. Any insurance or self-insurance maintained by the COUNTY, its officers, agents, officials, employees or volunteers shall be excess of the CONSULTANT's insurance and shall not contribute with it.*
 - c. *Each insurance policy required by this agreement shall be endorsed to state that coverage shall not be canceled by either party, except with written notice to the COUNTY.*

d. CONSULTANT hereby grants to COUNTY a waiver of any right to subrogation which any insurer of CONSULTANT may acquire against the county by virtue of the payment of any loss under such insurance. CONSULTANT agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation, but this provision applies regardless of whether or not the COUNTY has received a waiver of subrogation endorsement from the insurer.

3. The Workers' Compensation policy shall be endorsed with a waiver of subrogation in favor of the COUNTY for all work performed by the CONSULTANT, its employees, agents and subcontractors. CONSULTANT waives all rights against the COUNTY and its officers, agents, officials, employees and volunteers for recovery of damages to the extent these damages are covered by the workers compensation and employers liability.

C. Deductibles and Self-Insured Retentions

Self-insured retentions must be declared and the COUNTY Risk Manager must approve any deductible or self-insured retention that exceeds \$100,000.

D. Acceptability of Insurance

Insurance must be placed with insurers with a current rating given by A.M. Best and Company of no less than A-:VII and a Standard & Poor's Rating (if rated) of at least BBB and from a company approved by the Department of Insurance to conduct business in California. Any waiver of these standards is subject to approval by the County Risk Manager.

E. Verification of Coverage

Prior to approval of this Agreement by the COUNTY, the CONSULTANT shall file with the submitting department, certificates of insurance with original endorsements effecting coverage in a form acceptable to the COUNTY. Endorsements must be signed by persons authorized to bind coverage on behalf of the insurer. The COUNTY reserves the right to require certified copies of all required insurance policies at any time.