BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement"), effective March 1, 2022 ("Effective Date"), is entered into by and between iland Internet Solutions Corporation (the "Provider") and San Bernardino County on behalf of Arrowhead Regional Medical Center, (the "Customer" and each a "Party" and collectively the "Parties").

RECITALS

WHEREAS, the Parties have entered into a master service agreement dated on or about the date of this Agreement (the "MSA") pursuant to which the Provider will provide certain cloud computing services (the "Services") to the Customer;

WHEREAS, in connection with the Services, Customer may disclose to Provider certain protected health information (as defined herein) ("PHI") that is subject to protection under applicable provisions of: (i) the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, as amended ("HIPAA"); (ii) the privacy standards (at 45 C.F.R. parts 160 and 164, subparts A and E (the "Privacy Rule")) and security standards (at 45 C.F.R. parts 160, 162 and 164, subpart C (the "Security Rule")) adopted by the U.S. Department of Health and Human Services ("HHS"); (iii) Subtitle D of the Health Information Technology for Economic and Clinical Health Act, Pub. L 111- 5 (the "HITECH Act"); and (iv) the breach notification standards for unsecured PHI (at 45 C.F.R. parts 160 and 164, subparts A and D (the "Breach Notification Rule")) adopted by HHS, all as they may be amended from time to time (collectively, the "HIPAA Rules");

WHEREAS, the HIPAA Rules require that Customer receive assurances that Provider will comply with applicable obligations under the HIPAA Rules with respect to any PHI on received from or on behalf of Customer in the course of providing Services to Customer; and

WHEREAS the purpose of this Agreement is to comply with the requirements of the HIPAA Rules.

NOW THEREFORE, in consideration of the mutual promises and covenants herein, and for other good and valuable consideration the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

A. Definitions. Terms used herein, but not otherwise defined, shall have meaning ascribed by the HIPAA Rules.

1. Breach. "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. Breach excludes: (a) any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of Customer or Provider that is made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule; (b) any inadvertent disclosure by a person who is authorized to access PHI at Customer or Provider to another person authorized to access PHI at Customer or Provider, or organized health care arrangement in which Customer participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; or (c) a disclosure of PHI where Customer or Provider has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2. Designated Record Set. "Designated Record Set" means a group of records maintained by or for Customer that is: (i) the medical records and billing records about individuals maintained by or for Customer (if Customer is a health care provider under the Privacy Rule); (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about individuals. For purposes of this definition, the term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for Customer.

3. Individual. "Individual" shall mean the person who is the subject of the PHI.

4. Protected Health Information ("PHI") . "Protected Health Information" or PHI shall mean individually identifiable health information that is transmitted or maintained in any form or medium.

5. Required by Law. "Required by Law" shall mean a mandate contained in law that compels a use or disclosure of PHI.

6. Security Incident. "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.

7. Secretary. "Secretary" means the Secretary of the U.S. Department of Health and Human Services or his or her designee.

8. Services. "Services" has the meaning ascribed such term in the MSA.

9. Unsecured Protected Health Information ("Unsecured PHI"). "Unsecured Protected Health Information" or "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. Purposes for which PHI May Be Disclosed to Provider. Customer may disclose PHI to Provider in order to permit Provider to provide the Services.

C. Obligations of Customer. If relevant to Provider's responsibilities hereunder, Customer shall:

1. provide Provider a copy of its Notice of Privacy Practices ("Notice") as well as any changes to such Notice;

2. notify Provider of any restriction to the use and/or disclosure of an individual's PHI to which Customer has agreed in accordance with the Privacy Rule;

3. notify Provider of any amendment to an individual's PHI to which Customer has agreed that affects Provider's use and/or disclosure of a Designated Record Set in the custody and control of Provider; and

4. if Provider maintains a Designated Record Set, provide Provider with a copy of Customer's policies and procedures related to an individual's right to: access PHI; request an amendment to PHI; request confidential communications of PHI; or request an accounting of disclosures of PHI.

D. Obligations of Provider. Provider agrees to comply with applicable provisions of the HIPAA Rules, including:

1. Use and Disclosure of PHI. Except as otherwise permitted by this Agreement or the HIPAA Rules, Provider shall use or disclose PHI only as necessary to provide the Services to or on behalf of Customer. Provider's use and disclosure of PHI must comply with applicable requirements of 42 C.F.R. § 164.504(e) and Provider may not use or disclose PHI in a manner that would violate the Privacy Rule if used or disclosed by Customer. Provided, however, Provider may use and disclose PHI for the

proper management and administration of Provider, or to carry out its legal responsibilities. Provider shall in such cases:

(a) provide information to members of its workforce using or disclosing PHI regarding the obligations of Provider under the HIPAA Rules and this Agreement; and

(b) obtain reasonable assurances from the person or entity to whom the PHI is disclosed that: (i) the PHI will be held confidential and further used and disclosed only as required by law or for the purpose for which it was disclosed to the person or entity; and (ii) the person or entity will notify Provider of any instances of which it is aware in which confidentiality of the PHI has been breached.

2. Data Aggregation. In the event that Provider works for more than one covered entity, Provider may use and disclose PHI for data aggregation purposes, however, only in order to analyze data for permitted health care operations, and only to the extent that such use is permitted under the Privacy Rule.

3. Notice to Customer of Unauthorized Use or Disclosure or a Security Incident. Every reasonably suspected and actual Breach shall be reported promptly, but no later than ten (10) business days after discovery, to Customer's Office of Compliance, consistent with the regulations under HITECH Act. Upon discovery of a Breach or suspected Breach, Provider shall complete the following actions:

(a) Provide Customer's Office of Compliance with the following information to include but not limited to:
  (i) Date the Breach or suspected Breach occurred;
  (ii) Date the Breach or suspected Breach was discovered;
  (iii) Number of Provider staff, employees, subcontractors, agents or other third parties involved; and
  (iv) Description of how the Breach or suspected Breach allegedly occurred.

(b) Provide a completed risk assessment and investigation documentation to Customer's Office of Compliance within ten (10) business days of discovery of the Breach or suspected Breach with a determination as to whether a Breach has occurred. At the reasonable discretion of Customer, additional information may be requested.

(c) Make available to Customer and governing State and Federal agencies in a time and manner designated by Customer or governing State and Federal agencies, any policies, procedures, internal

practices and records reasonably relating to a Breach or reasonably suspected Breach for the purposes of audit.

4. Notice to Customer of Breach of Unsecured Protected Health Information. If Provider discovers that a breach of unsecured PHI has occurred, Provider shall notify Customer without unreasonable delay and in no case later than ten (10) business days after Provider's discovery of the breach. In its notice to Customer, Provider shall provide, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by Provider to have been, accessed, acquired, used, or disclosed during the breach. Provider shall provide any other available information that Customer is required to include in notification to the individual under the Breach Notification Rule at the time of the notice or promptly thereafter as information becomes available, including but not limited to: (i) a brief description of what happened, including the date of the breach and the date of discovery of the breach; and (ii) a description of the types of unsecured PHI that were involved in the breach.

5. Marketing/Fundraising. Provider shall not, without written authorization from Customer, perform marketing or fundraising on behalf of Customer, or engage in the types of communications on behalf of Customer that are excepted from the definition of marketing established at 45 C.F.R. § 164.501.

6. No Sale of Protected Health Information. Provider shall not directly or indirectly receive remuneration in exchange for an individual's PHI unless it is pursuant to specific written authorization by the individual or subject to an exception established in the HIPAA Rules.

7. Implementation of Safeguards. Provider shall maintain appropriate safeguards to ensure that PHI is not used or disclosed other than as provided by this Agreement or as required by law. In accordance with the HITECH Act and applicable provisions of the Security Rule, Provider shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic PHI it creates, receives, maintains, or transmits on behalf of Customer.

8. Minimum Necessary. When using or disclosing PHI or when requesting PHI from another covered entity in accordance with the "minimum necessary" requirements of the Privacy Rule found at section 164.502(b) thereof, prior to the issuance of guidance by the Secretary on what constitutes "minimum necessary," to the extent practicable, Provider shall limit PHI to "limited data set" information as that term is defined at section 164.514(e)(2) of the Privacy Rule or, if needed, to the minimum necessary to accomplish the intended purpose of such use, disclosure or request; provided, however, that following the Secretary's issuance of guidance on what constitutes "minimum necessary" Provider's sole obligation will be to follow the "minimum necessary" obligations of the Privacy Rule and the relevant

guidance of the Secretary.

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

10. Internal Practices, Policies and Procedures. Provider shall make its practices, books and records related to use and disclosure of PHI available to the Secretary upon request for the purpose of determining Customer's compliance with this Agreement and the HIPAA Rules. Records requested that are not protected by a legal privilege will be made available in the time and manner specified by the Secretary. Provider shall confer with Customer regarding legal privilege(s) that may be asserted or waived on behalf of Customer.

11. Assumption of Customer Obligations. To the extent Provider carries out one or more obligations for Customer under 45 C.F.R. § 164, Subpart E, Provider shall comply with all standards and implementation specifications of such Subpart that apply to Customer in the performance of the obligation(s).

12. Accounting of Disclosures.

(a) Provider shall keep records of all disclosures of PHI made by Provider necessary for Provider to provide to Customer the disclosure accounting described below ("Disclosure Accounting") in accordance with 45 C.F.R. § 164.528.

(b) If an individual submits a request for a Disclosure Accounting to Provider, Provider shall promptly forward a copy of the request to Customer.

(c) Provider shall provide the Disclosure Accounting to Customer (or to an Individual, if so directed by Customer or an Individual makes a request directly to Provider) within twenty (20) business days of receiving a written request therefore. The Disclosure Accounting shall contain the following (or such other information as may be permitted consistent with 45 C.F.R. § 164.528:

(i) the date of the disclosure;

(ii) the name of the entity or person to whom or which the PHI was provided and, if known, the address of such entity or person;

(iii) a brief description of the PHI disclosed; and

(iv) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu of such statement, a copy of the applicable written request for information to which the disclosure was responsive.

13. Assistance in Litigation or Administrative Proceedings. Provider shall make itself, and any subcontractors, employees, or agents assisting Provider in the performance of its obligations under the Agreement, available to Customer, at Customer's expense, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Customer, 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 Provider or its subcontractor, employee or agent is a named adverse party.

E. Term and Termination.

1. Term. This Agreement shall be effective as of the Effective Date and shall be terminated when all PHI provided to Provider by Customer, or created or received by Provider on behalf of Customer, is destroyed or returned to Customer.

2. Termination for Breach. Either Customer or Provider may terminate this Agreement if either party determines that there has been a material breach or violation of the other party's obligations under this Agreement. At its option, either party may take reasonable steps to cure the breach or end the violation. If the breach or violation continues and termination of the Agreement is not feasible, the non-breaching party may report the problem to the Secretary.

3. Judicial or Administrative Proceedings. Customer may terminate this Agreement, effective immediately, if (i) Provider 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 Provider has been joined that the Provider has violated any standard or requirement of HIPAA, the HITECH Act, the Privacy Rule, Security Rule or other security or privacy laws.

4. Effect of Termination. Upon termination of this Agreement for any reason, Provider agrees to return or destroy all PHI received from Customer, or created or received by Provider on behalf of Customer, maintained by Provider in any form. If Provider determines that the return or destruction of PHI is not feasible, Provider shall inform Customer in writing of the reason thereof, and shall agree to extend the protections of this Agreement to such PHI and limit further uses and disclosures of the PHI to those purposes

that make the return or destruction of the PHI not feasible for so long as Provider retains the PHI.

5. Mitigation. If Provider violates this Agreement or the HIPAA Rules, the Parties shall mitigate any damage caused by such breach.

6. Survival. The respective rights and obligations of Provider under Section E.3 of this Agreement shall survive the termination of this Agreement.

F. Intentionally Omitted.

G. Miscellaneous.

1. Notices. Any notices pertaining to this Agreement shall be given in writing and shall be deemed duly given when personally delivered to a Party or a Party's authorized representative as listed below or sent by means of a reputable overnight carrier, sent by means of certified mail, return receipt requested, postage prepaid, or by email. A notice sent by certified mail shall be deemed given on the date of receipt or refusal of receipt. A notice sent by email to the Provider shall be sent to legal@iland.com with a physical copy sent to the Provider address below. All notices shall be addressed to the appropriate Party as follows:

If to Customer:
Arrowhead Regional Medical Center
400 N Pepper Ave
Colton, CA 92324

Attn: Director of Information Management

If to Provider:
1235 North Loop West, #800
Houston, TX 77008
Attn: General Counsel

2. Amendments. This Agreement may not be changed or modified in any manner except by an instrument in writing signed by a duly authorized officer of each of the Parties hereto. Notwithstanding the foregoing. to the extent that any relevant provision of HIPAA or the HIPAA Rules is amended in a manner that changes the obligations of Provider or Customer provided for in this Agreement, such changes shall be deemed automatically to apply to and to be incorporated by reference into this Agreement. The Parties agree to amend this Agreement from time to time as necessary to reflect their agreement to such changes.

3. Severability. The provisions of this Agreement shall be severable, and if any provision of this Agreement shall be held or declared to be illegal, invalid or

unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

4. No Third Party Beneficiaries. Nothing in this Agreement shall be considered or construed as conferring any right or benefit on a person not party to this Agreement nor imposing any obligations on either Party hereto to persons not a party to this Agreement.

5. Entire Agreement. This Agreement, including the Business Associate Addendum for Cloud Services, as attached hereto as Attachment A and incorporated herein, together with all Exhibits, Riders and amendments, if applicable, which are fully completed and signed by authorized persons on behalf of both Parties from time to time while this Agreement is in effect, constitutes the entire Agreement between the Parties hereto with respect to the subject matter hereof and supersedes all previous written or oral understandings, Agreements, negotiations, commitments, and any other writing and communication by or between the Parties with respect to the subject matter hereof. In the event of any inconsistencies between any provisions of this Agreement in any provisions of the Exhibits, Riders, or amendments, the provisions of this Agreement shall control.

6. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Customer and Provider to comply with the HIPAA Rules. The provisions of this Agreement shall prevail over the provisions of any other Agreement that exists between the Parties that may conflict with, or appear inconsistent with, any provision of this Agreement or the HIPAA Rules.

7. No Agency. Provider shall not be deemed to be the common law agent of Customer as a result of this Agreement.

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

9. Compliance with State Law. In addition to HIPAA and all applicable HIPAA Regulations, Provider acknowledges that Provider and Customer 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 Agreement or HIPAA Regulations or the HITECH Act conflict with CMIA or any other California State law regarding the degree of protection provided for PHI and patient medical records, then Provider shall comply with the more restrictive requirements.

H. This Agreement may be executed in any number of counterparts, each of which so executed shall be deemed to be an original, and such counterparts shall together constitute one and the same Agreement. The parties shall be entitled to sign and

transmit an electronic signature of this Agreement (whether by facsimile, PDF or other email transmission), which signature shall be binding on the party whose name is contained therein. Each party providing an electronic signature agrees to promptly execute and deliver to the other party an original signed Agreement upon request.

[SIGNATURES ON NEXT PAGE]

Agreed to:

ILAND INTERNET SOLUTIONS CORPORATION

By: DocuSigned by: Brett Diamond D3F75F84B5814CE...
(Authorized Signature)

Name: Brett Diamond
(Type or Print)

Title: CEO

Date: 2/2/2022

SAN BERNARDINO COUNTY ON BEHALF OF ARROWHEAD REGIONAL MEDICAL CENTER

By: _____
(Authorized Signature)

Name: _____
(Type or Print)

Title: _____

Date: _____

ATTACHMENT A

Business Associate Addendum for Cloud Services

Backup as a Service (BaaS)

This Business Associate Addendum for Cloud Services ("Addendum") 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 ("Provider") to the Covered Entity ("Customer"). Capitalized terms shall have the same meaning as provided in the BAA. All capitalized terms used in this Addendum shall have the same meaning in the Provider's Master Service Agreement (the "Agreement") between the Provider and the Customer, unless expressly defined otherwise in this BAA or Addendum.

1) **DEFINITIONS:**
   a) **"Backup as a Service (BaaS)"** -- The cloud computing service where the Customer purchases backup and/or recovery services from a cloud hosting provider, such as the Provider. Customer does not manage or control the underlying physical cloud infrastructure including the servers, physical hosts, physical networks, data centers.
   b) "**Data**" - means any information, formulae, algorithms, or other content that Customer or Customer's employees, agents and end users not limited to upload, create publish, 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) **BaaS AVAILABILITY:** Unless otherwise stated in a Statement of Work (SOW):
   a) The Provider will provide BaaS availability in accordance with the Provider's Service Level Agreement ("SLA") reference in the Agreement and located at https://iland.com/legal/sla
   b) If the BaaS Availability in Section 1 of the Provider's SLA averages less than 98% of an Order for three (3) months over a rolling twelve (12) month period, the Customer may terminate the affected Order by providing the Provider a thirty (30) day advance written notice in the Provider's Customer Hub located at https://success.iland.com/home

3) **DATA SECURITY:**
   a) During the Term of any Order(s) issued under this Agreement, Provider will maintain an information security program designed to provide at least the same level of protection as evidenced by the controls described in the Provider's System and Organization Controls 2, Type 2 Report (the "SOC2 Report") in place on the Effective

Date or a successor or such alternative industry standard reports or certifications that are substantially and materially equivalent as reasonably determined by the Provider. Provider will make this documentation available to the Customer in the Provider's Customer Hub or any other method that the Provider reasonably deems to be sufficient and this documentation will be treated as Confidential Information of the Provider.

b) No Data shall be copied, modified, destroyed, published, or deleted by Provider other than for (1) normal operation or maintenance of BaaS during the Addendum or (2) as provided in the Agreement without prior written notice to and written approval by Customer.

c) Provider shall provide access to Data only to those employees, contractors and subcontractors who need to access the Data to fulfill Provider's obligations under this Agreement. Provider 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.

4) **ENCRYPTION:** In the event that the Customer procures services from the Provider in which the Provider provides encryption, the Provider shall provide that encryption in accordance with the Provider's Service Schedule located at https://www.iland.com/legal/service-schedule

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

6) **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 Customer, and Provider has a limited, non-exclusive license to access and use the Data as provided to Provider solely for performing its obligations under the BAA and the Agreement. 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 Provider 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.

7) **TRANSITION PERIOD**: Upon termination of an Order, the Customer may request and prepay for a period in which the Provider will not destroy the Data ("Prepaid Period"). The Customer may also request that the Provider assist with the migration with the Customer's data prior to the termination of an Order or during a Prepaid Period, and any such assistance provider by the Provider shall be at the Customer's expense.

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