THE INFORMATION IN THIS BOX IS NOT A PART OF THE CONTRACT AND IS FOR COUNTY USE ONLY

SAN BERNARDINO COUNTY

Contract Number

23-577 A1

SAP Number
4400022870

Arrowhead Regional Medical Center

Department Contract Representative	**Andrew Goldfrach**
Telephone Number	**(909) 580-6150**
Contractor	**InvisAlert Solutions, Inc.**
Contractor Representative	Andrew Jones
Telephone Number	(801) 819-4488
Contract Term	July 1, 2023 through June 30, 2028
Original Contract Amount	$285,125
Amendment Amount	N/A
Total Contract Amount	$285,125
Cost Center	
Grant Number (if applicable)	N/A

AMENDMENT NO. 1

WHEREAS, San Bernardino County on behalf of Arrowhead Regional Medical Center ("Purchaser") and InvisAlert Solutions, Inc. ("InvisAlert") entered into a License and Services Agreement ("Agreement") fully executed on June 27, 2023; and

WHEREAS, the parties now desire to incorporate a Business Associate Agreement ("BAA") into the Agreement; and

NOW THEREFORE, effective as of the date this Amendment is fully executed, the Agreement is amended as follows:

1. Section 1 of the Agreement is deleted in its entirety and replaced with the following:

    1. General Provision. This Agreement is comprised of the following elements:

        a) General Terms and Conditions.
        b) Attachment A – Insurance Requirements.

c) Schedule 1 Licensed Software.
d) Schedule 2 Implementation Services.
e) Schedule 3 Support Services.
f) Schedule 4 Fee Structure
g) ordering Document(s), set forth in Schedule 5
h) Exhibit A - Business Associate Agreement
i) Exhibit B – Levine Act – Campaign Contribution Disclosure

2. Section 11 of the General Terms and Conditions of the Agreement is deleted in its entirety and replaced with the following:

> **11. Individually Identifiable Health Information.** Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, regulations have been promulgated governing the privacy of individually identifiable health information. The HIPAA Privacy Rule and Security Rule specify requirements with respect to contracts between a Covered Entity and its Business Associates. InvisAlert shall comply with the attached Business Associate Agreement (Exhibit A). InvisAlert further agrees to comply with the requirements of other federal and state law that applies to the information collected and maintained by InvisAlert for services performed pursuant to Agreement.

3. Exhibit A of this Amendment is incorporated into the Agreement.

4. **Levine Act - Campaign Contribution Disclosure (formerly referred to as Senate Bill 1439)**

   InvisAlert has disclosed to the Purchaser using Exhibit B – Levine Act - Campaign Contribution Disclosure (formerly referred to as Senate Bill 1439), attached hereto, whether it has made any campaign contributions of more than $500 to any member of the San Bernardino County ("County") Board of Supervisors or other County elected officer [Sheriff, Assessor-Recorder-Clerk, Auditor-Controller/Treasurer/Tax Collector and the District Attorney] within the 12 months before the date this Amendment was approved by the Board of Supervisors. InvisAlert acknowledges that under Government Code section 84308, InvisAlert is prohibited from making campaign contributions of more than $500 to any member of the Board of Supervisors or other County elected officer for 12 months after the County's consideration of the Amendment.

   In the event of a further proposed amendment to the Agreement, InvisAlert will provide the County a written statement disclosing any campaign contribution(s) of more than $500 to any member of the Board of Supervisors or other County elected officer within the preceding 12 months of the date of the proposed amendment.

   Campaign contributions include those made by any agent/person/entity on behalf of InvisAlert or by a parent, subsidiary or otherwise related business entity of InvisAlert.

5. Exhibit B of this Amendment is incorporated into the Agreement.

6. **Full Force and Effect**. All other terms and conditions of the Agreement remain in full force and effect.

7. **Capitalized Terms**. Any capitalized term used but not defined in this Amendment shall have the meaning given to it in the Agreement.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

8. **Electronic Signatures**. This Amendment 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 Amendment. The parties shall be entitled to sign and transmit an electronic signature of this Amendment (whether by facsimile, PDF or other mail transmission), which signature shall be binding on the party whose name is contained therein. Each party providing an electronic signature agrees to promptly execute and deliver to the other party an original signed Amendment upon request.

IN WITNESS WHEREOF, San Bernardino County on behalf of Arrowhead Regional Medical Center and InvisAlert Solutions, Inc. have each caused this Amendment to be subscribed by its respective duly authorized officers, on its behalf.

SAN BERNARDINO COUNTY ON BEHALF OF ARROWHEAD REGIONAL MEDICAL CENTER

► Dawn Rowe

Dawn Rowe, Chair, Board of Supervisors

Dated: MAR 10 2026

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
San Bernardino County

By _____ Deputy

INVISALERT SOLUTIONS, INC.

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

By DocuSigned by: Ross Leo
348D4F27B7C84D8...
(Authorized signature - sign in blue ink)

Name Ross Leo
(Print or type name of person signing contract)

Title CISO
(Print or Type)

Dated: 01/29/2026

Address 21 West Washington St. Suite E/F

Wester Chester, PA 19380

FOR COUNTY USE ONLY

Approved as to Legal Form
► _____
Charles Phan, Supervising Deputy County Counsel
Date 2/5/2026

Reviewed for Contract Compliance
► _____
Date _____

Reviewed/Approved by Department
► _____
Andrew Goldfrach, ARMC Chief Executive Officer
Date 2/6/2026

EXHIBIT A

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") supplements and is made a part of the License and Services Agreement ("Contract") fully executed on June 27, 2023 by and between the San Bernardino County on behalf of Arrowhead Regional Medical Center (hereinafter Covered Entity) and InvisAlert Solutions, Inc. (hereinafter "Business Associate"). This Agreement 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:

I. Definitions

Unless otherwise specified herein, capitalized terms used in this Agreement 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.

a. 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.

b. 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.

c. 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.

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

e. 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.

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

g. 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.

h. 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.

i. 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.

j. 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).

II. Obligations and Activities of BA

a. 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 Agreement 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)]

b. Prohibited Uses and Disclosures

i. BA shall not use, access or further disclose PHI other than as permitted or required by this Agreement and as specified in the attached Contract or as required by law. Further, 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 Agreement.

c. 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 Agreement.

d. 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.

e. 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:

1. Date the Breach or suspected Breach occurred;
2. Date the Breach or suspected Breach was discovered;
3. Number of staff, employees, subcontractors, agents or other third parties and the names and titles of each person allegedly involved;
4. Number of potentially affected Individual(s) with contact information; and
5. 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:

1. The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;
2. The unauthorized person who had access to the PHI;
3. Whether the PHI was actually acquired or viewed; and
4. 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.

1. If BA and CE agree that a Breach has not occurred, notification to Individual(s) is not required.
2. 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.

f. 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.

g. 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.

h. 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.

i. 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.

j. Termination

CE may immediately terminate this agreement, and any related agreements, if CE determines that BA has breached a material term of this agreement. 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.

k. Return of PHI

Upon termination of this Agreement, 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 Agreement, to any PHI retained by BA or its subcontractors, employees or agents after the termination of this Agreement, and to limit any further use, access or disclosures.

l. 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 Agreement, 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.

m. 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 Agreement.

n. 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 the Agreement 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.

o. 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.

p. 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.

q. 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.

r. 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 Agreement 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 Agreement and under HIPAA 45 C.F.R. Parts 160 and 164, Subparts A and E.

s. 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 Agreement, 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.

III. **Obligations of CE**

a. 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.

IV. **General Provisions**

a. 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.

b. Ownership

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

c. Regulatory References

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

d. No Third-Party Beneficiaries

Nothing express or implied in the Contract or this Agreement 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.

e. Amendment

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

f. Interpretation

Any ambiguity in this Agreement shall be resolved to permit CE to comply with the Privacy and Security Rules, the HITECH Act, and all applicable patient confidentiality regulations.

g. Compliance with State Law

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 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 BA shall comply with the more restrictive requirements.

h. 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 Agreement.

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

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

1. DEFINITIONS:

a) "**Software as a Service (SaaS)**" - The capability provided to the consumer is to use applications made available by the provider running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser or application. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

b) "**Data**" - means any information, formulae, algorithms, or other content that the County, the County's employees, agents and end users upload, create or modify using the SaaS pursuant to this Contract. Data also includes user identification information, Protected Health Information (as defined by the Health Insurance Portability and Accountability Act (HIPAA)) and metadata which may contain Data or from which the Data may be ascertainable.

c) "**Data Breach**" - means any access, destruction, loss, theft, use, modification or disclosure of Data by an unauthorized party or that is in violation of Contract terms and/or applicable state or federal law.

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

a) The SaaS shall be available twenty-four (24) hours per day, 365 days per year (excluding agreed-upon maintenance downtime).

b) If SaaS monthly availability averages less than 99.5% (excluding agreed-upon maintenance downtime), the County shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the SOW.

c) If SaaS monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the County may terminate the contract for material breach.

d) Contractor shall provide advance written notice to the County in the manner set forth in the SOW of any major upgrades or changes that will affect the SaaS availability.

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

a) The Data shall be available twenty-four (24) hours per day, 365 days per year (excluding agreed-upon maintenance downtime).

b) If Data monthly availability averages less than 99.5% (excluding agreed-upon maintenance downtime), the County shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the SOW if the County is unable to access the Data as a result of:

1) Acts or omissions of Contractor;

2) Acts or omissions of third parties working on behalf of Contractor;

3) Network compromise, network intrusion, hacks, introduction of viruses, disabling devices, malware and other forms of attack that can disrupt access to Contractor's server, to the extent such attack would have been prevented by Contractor taking reasonable industry standard precautions;
4) Power outages or other telecommunications or Internet failures, to the extent such outages were within Contractor's direct or express control.

c) If Data monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the County may terminate the contract for material breach.

4. DATA SECURITY:

a) In addition to the provisions set forth in the Business Associate Agreement, Contractor shall certify to the County:
1) The sufficiency of its security standards, tools, technologies and procedures in providing SaaS under this Contract;
2) Compliance with the following:
i. The California Information Practices Act (Civil Code Sections 1798 et seq.);
ii. Undergo an annual Statement on Standards for Attestation Engagements (SSAE) 18 Service Organization Control (SOC) 2 Type II audit. Audit results and Contractor's plan to correct any negative findings shall be made available to the County within thirty (30) business days of Contractor's receipt of such results.
iii. Alternatively and in lieu of the SOC report noted above, the Contractor may submit a HITRUST CSF Validated Certification Report indicating successful attainment of HITRUST Certification, the scope of which must include HIPAA regulatory requirements. Similarly, examination results and Contractor's plan to correct any negative findings shall be made available to the County within thirty (30) business days of Contractor's receipt of such results.
iv. In the case of (iii) above, the Contractor shall also submit the equivalent report (either SOC 2 Type II, or HITRUST CSF certification) held by its subcontractor(s).

b) Contractor shall implement and maintain all appropriate administrative, physical, technical and procedural safeguards in accordance with section a) above at all times during the term of this Addendum to secure such Data from Data Breach, protect the Data and the SaaS from hacks, introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the County's access to its Data.

c) Contractor shall allow the County reasonable access to SaaS security logs, latency statistics, and other related SaaS security data that affect this Addendum and the County's Data, at no cost to the County.

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

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

f) Contractor shall provide access to Data only to those employees, contractors and subcontractors who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor will ensure that, prior to being granted access to Data, staff who perform work under this agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all data protection provisions of this Addendum and the associated Business Associate Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

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

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

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

8. TRANSITION PERIOD:

a) For ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Contractor shall assist the County in extracting and/or transitioning all Data in the format determined by the County ("Transition Period").
b) The Transition Period may be modified in the SOW or as agreed upon in writing by the parties in a contract amendment.
c) During the Transition Period, SaaS and Data access shall continue to be made available to the County without alteration.
d) Contractor agrees to compensate the County for damages or losses the County incurs as a result of Contractor's failure to comply with this section.
e) Unless otherwise stated in the SOW, the Contractor shall permanently destroy or render inaccessible any portion of the Data in Contractor's and/or subcontractor's possession or control following the expiration of all obligations in this section. Within thirty (30) days, Contractor shall issue a written statement to the County confirming the destruction or inaccessibility of the County's Data.
f) The County at its option, may purchase additional transition services as agreed upon in the SOW.

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

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

Failure to do so may result in the County exercising its options for assessing damages or other remedies.

d) Contractor shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with the County. The County and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Contractor shall cooperate fully with the County, its agents and law enforcement.

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

a) Upon advance written request, Contractor agrees that the County or its designated representative shall have access to Contractor's SaaS operational documentation and records, including online inspections that relate to the security of the SaaS product purchased by the County.

b) Contractor shall allow the County, its authorized agents, or a mutually acceptable third party to test that controls are in place and working as intended. Tests may include, but not be limited to, the following:
   1) Operating system/network vulnerability scans,
   2) Web application vulnerability scans,
   3) Database application vulnerability scans, and
   4) Any other scans to be performed by the County or representatives on behalf of the County.

c) After any significant Data loss or Data Breach or as a result of any disaster or catastrophic failure, Contractor will at its expense have an independent, industry-recognized, County-approved third party perform an information security audit. The audit results shall be shared with the County within seven (7) days of Contractor's receipt of such results. Upon Contractor receiving the results of the audit, Contractor will provide the County with written evidence of planned remediation within thirty (30) days and promptly modify its security measures in order to meet its obligations under this Contract.

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

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

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

EXHIBIT B
Levine Act –
Campaign Contribution Disclosure
(formerly referred to as Senate Bill 1439)

The following is a list of items that are not covered by the Levine Act. A Campaign Contribution Disclosure Form will not be required for the following:

- Contracts that are competitively bid and awarded as required by law or County policy
- Contracts with labor unions regarding employee salaries and benefits
- Personal employment contracts
- Contracts under $50,000
- Contracts where no party receives financial compensation
- Contracts between two or more public agencies
- The review or renewal of development agreements unless there is a material modification or amendment to the agreement
- The review or renewal of competitively bid contracts unless there is a material modification or amendment to the agreement that is worth more than 10% of the value of the contract or $50,000, whichever is less
- Any modification or amendment to a matter listed above, except for competitively bid contracts.

DEFINITIONS

Actively supporting or opposing the matter: (a) Communicate directly with a member of the Board of Supervisors or other County elected officer [Sheriff, Assessor-Recorder-Clerk, District Attorney, Auditor-Controller/Treasurer/Tax Collector] for the purpose of influencing the decision on the matter; or (b) testifies or makes an oral statement before the County in a proceeding on the matter for the purpose of influencing the County's decision on the matter; or (c) communicates with County employees, for the purpose of influencing the County's decision on the matter; or (d) when the person/company's agent lobbies in person, testifies in person or otherwise communicates with the Board or County employees for purposes of influencing the County's decision in a matter.

Agent: A third-party individual or firm who, for compensation, is representing a party or a participant in the matter submitted to the Board of Supervisors. If an agent is an employee or member of a third-party law, architectural, engineering or consulting firm, or a similar entity, both the entity and the individual are considered agents.

Otherwise related entity: An otherwise related entity is any for-profit organization/company which does not have a parent-subsidiary relationship but meets one of the following criteria:

(1) One business entity has a controlling ownership interest in the other business entity;
(2) there is shared management and control between the entities; or
(3) a controlling owner (50% or greater interest as a shareholder or as a general partner) in one entity also is a controlling owner in the other entity.

For purposes of (2), "shared management and control" can be found when the same person or substantially the same persons own and manage the two entities; there are common or commingled funds or assets; the business entities share the use of the same offices or employees, or otherwise share activities, resources or personnel on a regular basis; or there is otherwise a regular and close working relationship between the entities.

Parent-Subsidiary Relationship: A parent-subsidiary relationship exists when one corporation has more than 50 percent of the voting power of another corporation.

Contractors must respond to the questions on the following page. The term "Contractor" on this Exhibit refers to InvisAlert. If a question does not apply respond N/A or Not Applicable.

1. Name of Contractor: Invisalert Solutions, Inc.

2. Is the entity listed in Question No.1 a nonprofit organization under Internal Revenue Code section 501(c)(3)?

   Yes ☐ If yes, skip Question Nos. 3-4 and go to Question No. 5 No x
   ☐

3. Name of Principal (i.e., CEO/President) of entity listed in Question No. 1, if the individual actively supports the matter and has a financial interest in the decision: ____Pete Nagy

4. If the entity identified in Question No.1 is a corporation held by 35 or less shareholders, and not publicly traded ("closed corporation"), identify the major shareholder(s):

   N/A

5. Name of any parent, subsidiary, or otherwise related entity for the entity listed in Question No. 1 (see definitions above):

Company Name	Relationship
N/A	

6. Name of agent(s) of Contractor:

Company Name	Agent(s)	Date Agent Retained (if less than 12 months prior)
N/A		

7. Name of Subcontractor(s) (including Principal and Agent(s)) that will be providing services/work under the awarded contract if the subcontractor (1) actively supports the matter and (2) has a financial interest in the decision and (3) will be possibly identified in the contract with the County or board governed special district.

Company Name	Subcontractor(s):	Principal and//or Agent(s):
N/A		

8. Name of any known individuals/companies who are not listed in Questions 1-7, but who may (1) actively support or oppose the matter submitted to the Board and (2) have a financial interest in the outcome of the decision:

Company Name	Individual(s) Name
N/A	

9. Was a campaign contribution, of more than $500, made to any member of the San Bernardino County Board of Supervisors or other County elected officer within the prior 12 months, by any of the individuals or entities listed in Question Nos. 1-8?

   No X☐ If **no**, please skip Question No. 10.

   Yes ☐ If **yes**, please continue to complete this form.

10. Name of Board of Supervisor Member or other County elected officer: _____

    Name of Contributor: _____

    Date(s) of Contribution(s): _____

    Amount(s): _____

    Please add an additional sheet(s) to identify additional Board Members or other County elected officers to whom anyone listed made campaign contributions.

By signing the Amendment, Contractor certifies that the statements made herein are true and correct. Contractor understands that the individuals and entities listed in Question Nos. 1-8 are prohibited from making campaign contributions of more than $500 to any member of the Board of Supervisors or other County elected officer while award of this Amendment is being considered and for 12 months after a final decision by the County.