California Integrated Vital Records System (Cal-IVRS)
Facility Participant Agreement

This California Integrated Vital Records System (Cal-IVRS) Data Privacy and Security Agreement ("Agreement") sets forth the data privacy and security requirements that San Brenardino County on behalf of Arrowhead Regional Medical Center [name of organization] ("Participant"), and the California Department of Public Health ("CDPH") are obligated to follow with respect to all Cal-IVRS Data (as defined herein). Permission for Participant to access, use, and disclose Cal-IVRS Data requires execution of this Agreement by Participant and CDPH.

I. Supersession: This Agreement supersedes any prior Cal-IVRS Agreement, or other agreement concerning Cal-IVRS Data, between CDPH and Participant.

II. Definitions: For purposes of this Agreement, the following definitions shall apply:

A. Breach: "Breach" means:

1. The acquisition, access, use, or disclosure of Cal-IVRS Data in violation of any state or federal law or in a manner not permitted under this Agreement that compromises the privacy, security or integrity of the information. For purposes of this definition, "compromises the privacy, security or integrity of the information" means poses a significant risk of financial, reputational, or other harm to an individual or individuals; or

2. The same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29, subdivision (f). The "system" referenced in Civil Code section 1798.29 shall be interpreted for purposes of this Agreement to reference the California Integrated Vital Records System (Cal-IVRS), only.

B. Cal-IVRS Data: "Cal-IVRS Data" means: All data that resides in the following CDPH information technology systems/databases:

1. Vital Records Business Intelligence System (VRBIS).

2. Electronic Birth Registration System (EBRS).

3. Electronic Death Registration System (EDRS).

4. Fetal Death Registration System (FDRS).

C. Disclosure: "Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of Cal-IVRS Data.

D. Personal Information: "Personal information" means information, in any medium (paper, electronic, oral) that:

1. directly or indirectly collectively identifies or uniquely describes an individual; or

2. could be used in combination with other information to indirectly identify or uniquely describe an individual, or link an individual to the other information; or

3. meets the definition of "personal information" set forth in California Civil Code section 1798.3, subdivision (a) or

4. is one of the data elements set forth in California Civil Code section 1798.29, subdivision (g)(1) or (g)(2); or

5. meets the definition of "medical information" set forth in either California Civil Code section 1798.29, subdivision (h)(2) or California Civil Code section 56.05, subdivision (j); or

6. meets the definition of "health insurance information" set forth in California Civil Code section 1798.29, subdivision (h)(3); or

7. is protected from disclosure under applicable state or federal law.

E. Security Incident: "Security Incident" means:

1. An attempted breach that results in a root cause analysis or forensics evaluation.

2. The attempted or successful modification or destruction of Cal-IVRS Data in the California Integrated Vital Records System in violation of any state or federal law or in a manner not permitted under this Agreement;

3. An event constituting a violation or imminent threat of violation of information security policies or procedures, including acceptable use policies; or

4. The attempted or successful modification or destruction of, or interference with, system operations in the California Integrated Vital Records System that negatively impacts the confidentiality, availability, or integrity of Cal-IVRS Data, or obstructs or makes impossible the receipt, collection, creation, storage, transmission or use of Cal-IVRS Data in the Cal-IVRS System.

F. Use: "Use" means the sharing, employment, application, utilization, examination, or analysis of Cal-IVRS Data.

G. Workforce Member: "Workforce Member" means an employee, volunteer, trainee, or other person whose conduct, in the performance of work for Participant, is under the direct control of Participant, whether or not they are paid by the Participant.

H. [Reserved.]

III. Background and Purpose: The CDPH and its Director, designated in statute as the State Registrar, pursuant to Division 102 of the California Health and Safety Code (H&SC), is charged with the duties of registering, maintaining, indexing and issuing certified copies of all California Birth, Death, and Fetal Death records. As part of these activities, the State Registrar operates the VRBIS, EBRS, EDRS, and FDRS databases. Responsibilities set forth in H&SC section 102247 and 102249 provide legislative direction to the State Registrar to develop and maintain an automation system for vital event registration, develop and maintain public health data bases, build a data system that will support policy analysis and program decisions at all levels, be useful to health care providers, local and community agencies, and the state to ultimately benefit consumers of health care services. VRBIS, EBRS, EDRS, and FDRS are necessary components to fulfilling these responsibilities.

A. VRBIS is a secure, web based electronic solution for the State Registrar to store California's vital records data and to permit Local Health Departments and others to access such data for purposes allowed under California statute, such as epidemiologic analysis, surveillance, and program evaluation, following all applicable laws and regulations concerning vital record data.

B. EBRS, EDRS, and FDRS are secure, web based electronic birth, death, and fetal death registration databases maintained by the State Registrar. Access to EBRS, EDRS, and FDRS is limited to statutorily defined record preparers, such as hospitals (section 102405,) funeral homes (sections 102780 and 102795,) and coroners (102850 – 102870,) as well as local registrars and the State Registrar, required by statute to register and preserve birth, death, and fetal death certificates. In EBRS, EDRS, and FDRS, record preparers enter certificate data into the registration database and electronically submit completed records to the local registrar to be registered. Once records are registered in EBRS, EDRS, and FDRS, record data are transmitted to VRBIS.

IV. Legal Authority: The legal authority for CDPH and Participant to collect, create, access, use

and disclose Cal-IVRS Data is set forth in Attachment A to this Agreement, which is made part of this Agreement by this reference.

V. Effect of the Health Insurance Portability and Accountability Act of 1996 (HIPAA):

A. CDPH and Cal-IVRS HIPAA Status: CDPH is a "hybrid entity" for purposes of applicability of the federal regulations entitled "Standards for Privacy of Individually Identifiable Health Information" ("Privacy Rule") (45 C.F.R. parts 160, 162, and 164) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. §§ 1320d - 1320d-8) (as amended by Subtitle D Privacy, of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111–5, 123 Stat. 265–66)). The Cal-IVRS System has not been designated by the CDPH as, and is not, one of the HIPAA-covered "health care components" of CDPH. (45 C.F.R. § 164.504(c)(3)(iii).) The legal basis for this determination is as follows:

1. The Cal-IVRS System is not a component of CDPH that would meet the definition of a covered entity or business associate if it were a separate legal entity. (45 C.F.R. §§ 160.105(a)(2)(iii)(D); 160.103 (definition of "covered entity").) And

2. The HIPAA Privacy Rule creates a special rule for a subset of public health activities whereby HIPAA cannot preempt state law if, "[t]he provision of state law, including state procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention." (45 C.F.R. § 160.203(c) [HITECH Act, § 13421, sub. (a)].) [NOTE: See State laws and regulations listed in Attachment A.

B. CDPH is a "Public Health Authority": CDPH is a "public health authority" as that term is defined in the Privacy Rule. (45 C.F.R. §§ 164.501; 164.512(b)(1)(i).)

C. Cal-IVRS Data Use and Disclosure Permitted by HIPAA: To the extent a disclosure or use of Cal-IVRS Data may also be considered a disclosure or use of "Protected Health Information" (PHI) of an individual, as that term is defined in part 160.103 of Title 45, Code of Federal Regulations, the following Privacy Rule provisions apply to permit such Cal-IVRS Data disclosure and/or use by CDPH and Participant, without the consent or authorization of the individual who is the subject of the PHI:

1. HIPAA cannot preempt state law if, "[t]he provision of state law, including state procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention." (45 C.F.R. § 160.203(c) [HITECH Act, § 13421, sub. (a)].) [NOTE: See state laws and regulations listed in Attachment A].

2. A covered entity may disclose PHI to a "public health authority" carrying out public health activities authorized by law; (45 C.F.R. § 164.512(b));

3. A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law." (Title 45 C.F.R. §§ 164.502 (a)(1)(vii), 164.512(a)(1).) And,

4. Other, non-public health-specific provisions of HIPAA may also provide the legal basis for all or specific Cal-IVRS Data uses and disclosures.

D. No HIPAA Business Associate Agreement or Relationship between CDPH and Participant: This Agreement and the relationship it memorializes between CDPH and Participant do not constitute a business associate agreement or business associate relationship pursuant to Title 45, CFR, part 160.103 (definition of "business associate"). The basis for this determination is part 160.203(c) of Title 45 of the Code of Federal Regulations (see, also, [HITECH Act, § 13421, subdivision. (a)].) [NOTE: See state laws and regulations listed in Attachment A]. Accordingly, this Agreement is not intended to nor at any time shall result in or be interpreted or construed as to create a business associate relationship between CDPH and Participant. By the execution of this Agreement, CDPH and Participant expressly disclaim the existence of any business associate relationship.

VI. Permitted Disclosures: The Participant and its workforce members and agents, shall safeguard the Cal-IVRS Data to which they have access to from unauthorized disclosure. The Participant, and its workforce members and agents, shall not disclose any Cal-IVRS Data for any purpose other than carrying out the Participant's obligations under the statutes and regulations set forth in Attachment A, or as otherwise allowed or required by state or federal law.

VII. Permitted Use: The Participant, and its workforce members and agents, shall safeguard the Cal-IVRS Data to which they have access to from unauthorized use. The Participant, and its workforce members and agents, shall not use any Cal-IVRS Data for any purpose other than carrying out the Participant's obligations under the statutes and regulations set forth in Attachment A or as otherwise allowed or required by state or federal law.

VIII. Safeguards: Participant shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of Cal-IVRS Data. The Participant shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Participant's operations and the nature and scope of its activities in performing its legal obligations and duties (including performance of its duties and obligations under this Agreement), and which incorporates the requirements of Section IX, Security, below. Participant shall provide CDPH with its current and updated policies within five (5) business days of a request by CDPH for the policies.

IX. Security: The Participant shall take all reasonable steps necessary to ensure the continuous security of all of Participant's computerized data systems that access, process, store, receive or transmit Cal-IVRS Data. These steps shall include, at a minimum, the following:

A. Providing a level and scope of security that is at least comparable to the level and scope of security established by the HIPAA Security Rule located at 45 C.F.R. Part 160 and Subparts A and C of Part 164.

X. Training: CDPH will provide training to Participant workforce members on the use of Cal-IVRS.

A. The Participant shall require each workforce member who receives training to receive and sign a certification, indicating the workforce member's name and the date on which the training was completed.

B. The Participant shall retain each workforce member's written certifications for CDPH inspection for a period of three years following contract termination.

XI. Participant Breach and Security Incident Responsibilities:

Notification to CDPH of Breach or Security Incident: The Participant shall notify CDPH immediately, by telephone call and email upon the discovery of a breach (as defined in this Agreement), and within twenty-four (24) hours by email of the discovery of any security incident (as defined in this Agreement), unless a law enforcement agency determines that the notification will impede a criminal investigation, in which case the notification required by this section shall be made to CDPH immediately after the law enforcement agency determines that such notification will not compromise the investigation. Notification shall be provided to the CDPH Privacy Officer and CDPH Chief Information Security Officer, using the contact information listed in Section XII(G), below. If the breach or security incident occurs after business hours or on a weekend or holiday and involves Cal-IVRS Data in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH Information Security Office at the telephone numbers listed in Section XII(G), below. For purposes of this Section, breaches and security incidents shall be treated as discovered by Participant as of the first day on which such breach or security incident is known to the Participant. Participant shall be deemed to have knowledge of a breach or security incident if such breach or security incident is known to any person, other than the person committing the breach or security incident, who is a workforce member or agent of the Participant.

Participant shall take:

1. prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the Cal-IVRS System operating environment; and,

2. Any action pertaining to a breach required by applicable federal or state laws,

and assist the Department in complying with California Civil Code section 1798.29.

B. Investigation of Breach: The Participant shall as soon as practicable, without unreasonable delay, investigate such breach or security incident, and shall make its best efforts to inform the CDPH Chief Information Security Officer within three business days of the discovery, of the following information, to the extent known:

1. what data elements were involved and the extent of the data involved in the breach, including, specifically, the number of individuals whose Personal Information was breached;

2. a description of the unauthorized persons known or reasonably believed to have improperly used the Cal-IVRS Data and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the Cal-IVRS Data, or to whom it is known (or reasonably believed) to have had the Cal-IVRS Data improperly disclosed to them;

3. a description of where the Cal-IVRS Data is known or believed to have been improperly used or disclosed;

4. a description of the known or probable causes of the breach or security incident; and

5. Whether Civil Code section 1798.29 or any other federal or state laws requiring individual notifications of breaches have been triggered.

C. Written Report: The Participant shall provide a written report of the investigation to the CDPH Program Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer within five (5) working days of the discovery of the breach or security incident. The report shall include, but not be limited to, the information specified above, as well as a corrective action plan, including information on measures that were taken to halt and/or contain the breach or security incident, and measures to be taken to prevent the recurrence of such breach or security incident.

D. Notification to Individuals: If notification to individuals whose information was breached is required under state or federal law, and regardless of whether Participant is considered only a custodian and/or non-owner of the Cal-IVRS Data, Participant shall cooperate with and assist CDPH in its notification (including substitute notification) to the individuals affected by the breach.

E. Submission of Sample Notification to California Attorney General: If notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29 due to a breach Participant is responsible for, Participant shall

1. Electronically submit a single sample copy of the security breach notification,

excluding any Personal Information, to the California Attorney General pursuant to the format, content and timeliness provisions of section 1798.29, subdivision (e). Participant shall inform the CDPH Privacy Officer of the time, manner and content of any such submissions, prior to the transmission of such submissions to the Attorney General; or

2. Cooperate with and assist CDPH in its submission of a sample copy of the notification to the California Attorney General.

F. Public Statements: Participant shall cooperate with CDPH in developing content for any public statements regarding Breaches or Security Incidents related to Participant. Requests for public statement(s) by any non-party about a breach or security incidents shall be directed to the CDPH Privacy Officer using the contact information listed in Section XII(G), below.

G. CDPH Contact Information: To direct communications to the above referenced CDPH staff, the Participant shall initiate contact as indicated below. CDPH reserves the right to make changes to the contact information by giving written notice to the Participant. Said changes shall not require an amendment to this Agreement.

CDPH Program Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer (and CDPH IT Service Desk)
Romeo Amian Assistant Deputy Director Center for Health Statistics and Informatics CA. Dept. of Public Health P.O. Box 997410, MS 5000 Sacramento, CA 95899-7410 Email: Romeo.Amian@cdph.ca.gov	**Privacy Officer** Privacy Office c/o Office of Legal Services CA Dept. of Public Health P.O. Box 997377, MS 0506 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	**Chief Information Security Officer** Information Security Office CA Dept. of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413 Email: CDPH.InfoSecurityOffice@cdph.ca.gov Telephone: (855) 500-0016

XII. CDPH Breach and Security Incident Responsibilities: CDPH shall notify Participant immediately by telephone call and email upon the discovery of a breach (as defined in this Agreement), or within twenty-four (24) hours by email of the discovery of any security incident (as defined in this Agreement) that involves Cal-IVRS Data that was created or collected by Participant in the Cal-IVRS System. Notification shall be provided by CDPH to the Participant Representative, using the contact information listed in Attachment B to this Agreement.

A. For purposes of this Section, breaches and security incidents shall be treated as

discovered by CDPH as of the first day on which such breach or security incident is known to CDPH, or, by exercising reasonable diligence would have been known to CDPH. CDPH shall be deemed to have knowledge of a breach or security incident if such breach or security incident is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach or security incident, who is a workforce member or agent of CDPH.

B. Participant Contact Information: To direct communications to the Participant's breach/security incident response staff, CDPH shall initiate contact as indicated by Participant in Attachment B. Participant's contact information must be provided to CDPH prior to execution of this Agreement. Participant reserves the right to make changes to the contact information in Attachment B. Such notice shall be provided to the CDPH Program Manager, the CDPH Privacy Officer or the CDPH Chief Information Security Officer, using the contact information listed in Section XII(G), above. Said changes shall not require an amendment to this Agreement.

XIII. Term of Agreement: Unless otherwise terminated earlier in accordance with the provisions set forth herein, this Agreement shall remain in effect for five (5) years after the latest signature date in the signature block below. After five (5) years, this Agreement will expire without further action. If the parties wish to extend this Agreement, they may do so by reviewing, updating, and reauthorizing this Agreement. If one or both of the parties wish to terminate this Agreement prematurely, they may do so upon 30 days' advance notice. CDPH may also terminate this Agreement pursuant to Section XIV, below.

XIV. Termination for Cause:

A. Termination upon Breach: A breach by Participant of any provision of this Agreement, as determined by CDPH, shall constitute a material breach of the Agreement and grounds for immediate termination of the Agreement by CDPH. At its sole discretion, CDPH may give Participant 30 days to cure the breach.

B. Judicial or Administrative Proceedings: Participant will notify CDPH if it is named as a defendant in a criminal proceeding related to a violation of this Agreement. CDPH may terminate the Agreement if Participant is found guilty of a criminal violation related to a violation of this Agreement. CDPH may terminate the Agreement if a finding or stipulation that the Participant has violated any security or privacy laws is made in any administrative or civil proceeding in which the Participant is a party or has been joined.

XV. Assistance in Litigation or Administrative Proceedings: Participant shall make itself and any workforce members or agents assisting Participant in the performance of its obligations under this Agreement available to CDPH at no cost to CDPH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CDPH, its director, officers or workforce members based upon claimed violation of laws relating to security and privacy, which involves inactions or actions by the Participant, except where Participant or its workforce member or agent is a named adverse party.

XVI. Disclaimer: CDPH makes no warranty or representation that compliance by Participant with this Agreement will be adequate or satisfactory for Participant's own purposes or that any information in Participant's possession or control, or transmitted or received by Participant, is or will be secure from unauthorized use or disclosure. Participant is solely responsible for all decisions made by Participant regarding the safeguarding of Cal-IVRS Data.

XVII. Transfer of Rights: Participant has no right and shall not delegate, assign, or otherwise transfer or delegate any of its rights or obligations under this Agreement to any other person or entity. Any such transfer of rights shall be null and void.

XVIII. No Third-Party Beneficiaries: Nothing express or implied in the terms and conditions of this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Participant, any rights, remedies, obligations or liabilities whatsoever.

XIX. Interpretation: The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with regulations and applicable State and Federal laws. The parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that complies and is consistent with Federal and State laws.

XX. Survival: The respective rights and obligations of Participant under Sections VIII, IX, XII, XIII, and XVIII of this Agreement shall survive the termination or expiration of this Agreement.

XXI. Attachments: The parties mutually agree that the following specified Attachments are part of this Agreement:

A. Attachment A: State Law Authority for: (1) Use and Disclosure of Cal-IVRS Data; and, (2) Application of HIPAA preemption exception for public health (45 C.F.R. § 160.203(c)).

B. Attachment B: Participant Breach and Security Incident Contact Information.

XXII. Entire Agreement: This Agreement, including all attachments, constitutes the entire agreement between CDPH and Participant. Any and all modifications of this Agreement must be in writing and signed by all parties. Any oral representations or agreements between the parties shall be of no force or effect.

XXIII. Severability: The invalidity in whole or in part of any provisions of this Agreement shall not void or affect the validity of any other provisions of this Agreement.

XXIV. Choice of Law and Venue: The laws of the state of California will govern any dispute from or relating to this Agreement. The parties submit to the exclusive jurisdiction of the state of California and federal courts for or in Sacramento and agree that any legal action or proceeding relating to the Agreement may only be brought in those courts.

XXV. Signatures:

IN WITNESS, WHEREOF, the Parties have executed this Agreement as follows:

On behalf of the Participant, the San Bernardino County on behalf of Arrowhead Regional Medical Center [name of organization], the undersigned individual hereby attests that they are authorized to enter into this Agreement and agrees to abide by and enforce all the terms specified herein.

Dawn Rowe
(Name of Representative of Participant)

Chair, Board of Supervisors
(Title)

(Signature) (Date)

On behalf of CDPH, the undersigned individual hereby attests that they are authorized to enter into this Agreement and agrees to all the terms specified herein.

Romeo Amian
(Name of CDPH Representative)

State Registrar/Deputy Director
(Title)

(Signature) (Date)

Return Executed Agreement to: California Department of Public Health
Attention: Cal-IVRS Support Desk
P.O. Box 997410, MS 5000
Sacramento, CA 95899-7410
EMAIL: cal-ivrs@cdph.ca.gov
FAX: 916-440-7357

Attachment A

Facility Participant

State Law Authority for:

(1) Use and Disclosure of Cal-IVRS Data; and,

(2) Application of HIPAA preemption exception for public health (45 C.F.R. § 160.203(c).

A. General Legal Authority:

1. California Information Practices Act:

   a. California Civil Code section 1798.24(e), provides in part as follows: “No agency may disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains unless the information is disclosed, as follows: To a person, or to another agency where the transfer is necessary for the transferee agency to perform its constitutional or statutory duties, and the use is compatible with a purpose for which the information was collected….”

B. Specific Legal Authority: Vital Records Collection, Use, and Dissemination

1. Division 102 of the California Health and Safety Code designates that the Director of CDPH is the State Registrar and such duties include the registration, preservation, and dissemination of all of California’s birth, death, and marriage records.

2. California Health and Safety Code section 102100 mandates the registration of each live birth, fetal death, death, and marriage that occurs in the state.

3. Pursuant to California Health and Safety Code section 102405, for live births that occur in a hospital, or a state-licensed alternative birth center, the attending physician and surgeon, certified nurse midwife, or principal attendant, or if the foregoing individuals are unavailable, the administrator of a hospital or center or a representative designated by the administrator in writing shall be responsible for certifying the live birth and registering the certificate with the local registrar.

4. Pursuant to California Health and Safety Code sections 102780 and 102955, a funeral director, or if there is no funeral director, the person acting in lieu thereof, shall prepare the death or fetal death certificate and register it with the local registrar.

5. California Health and Safety Code section 102230 designates that the State Registrar “shall arrange and permanently preserve the [vital records] certificates in a systematic manner and shall prepare and maintain comprehensive and continuous indices of all certificates registered.

6. Pursuant to California Health and Safety Code section 102430(a), the second section of the certificate of live birth as specified in subdivision (b) of California Health and Safety Code section 102425, the electronic file of birth information collected pursuant to subparagraphs (B) to (I), inclusive, of paragraph (2) of subdivision (a) of California Health and Safety Code section 102426, and the second section of the certificate of fetal death as specified in California Health and Safety Code section 103025, are confidential; however, access to this information is authorized for the following: the birth hospital responsible for preparing and submitting a record of the birth or fetal death for purposes of reviewing and correcting birth or fetal death records. The birth hospital shall not further disclose the information nor use the information for purposes other than as allowed by the California vital records laws.

Attachment B

Participant Breach and Security Incident Contact Information.

The following Participant contact information must be included in the executed Agreement

Participant Program Manager	**Participant Privacy Officer**	**Participant Chief Information Security Officer**
Leah Beck	Collin Goodrum	Robert Pittman
[Name] Health Information Management Director	[Name] Hospital Privacy Officer	[Name] Chief Information Security Officer
[Title] 1930 W. Valley Boulevard	[Title] 400 N. Pepper Avenue	[Title] 851 E. Cooley Drive
[Address]	[Address]	[Address]
[Address 2] Colton	[Address 2] Colton	[Address 2] Colton
[City] CA, 92324	[City] CA, 92324	[City] CA, 92324
[State, ZIP Code] (909) 658-3117	[State, ZIP Code] (909) 580-3287	[State, ZIP Code] (909) 388-5510
[Telephone] lbeck@armc.sbcounty.gov	[Telephone] goodrumc@armc.sbcounty.gov	[Telephone] Robert.Pittman@itd.sbcounty.gov
[E-mail]	[E-mail]	[E-mail]