EXHIBIT A

SJVIA CONSULTANT AGREEMENT

This agreement is dated _____ and is between [NAME OF CONSULTANT], a [type of entity] ("**Consultant**"), and the SAN JOAQUIN VALLEY INSURANCE AUTHORITY, a joint powers agency ("**SJVIA**").

The SJVIA is a joint exercise of powers authority that negotiates, purchases, or otherwise funds health, pharmacy, vision, and dental insurance (each an "**Insurance Program**," and collectively "**Insurance Programs**"). The SJVIA makes Insurance Programs available to participating entities, subject to the terms and conditions of an agreement by each participating entity to pay for its respective costs for the Insurance Programs in which it participates.

The SJVIA desires to retain the services of a consultant for health benefits consultation and administration services with specific experience in the public sector, risk-sharing pools, underwriting, self-funded health benefit plans, and the Affordable Care Act.

The Consultant represents and warrants to the SJVIA that it is ready, willing, and able to provide the services desired by the SJVIA subject to the terms and conditions of this agreement, and in cooperation with and under the direction of the SJVIA Board of Directors and SJVIA management.

The parties therefore agree as follows:

Article 1
Consultant's Obligations

1.1 **Scope of Services.** The Consultant shall perform all of the services described in Exhibit A to this agreement, titled "Scope of Services."

1.2 **Additional Services.** The Consultant may perform additional services as the SJVIA and the Consultant mutually agree in writing.

1.3 **Key Persons.** The Consultant shall perform all services under this agreement through the following key persons: [names and titles].

1.4 **Standard of Care.** The Consultant acknowledges that the SJVIA is governed by a board of local elected officials, and staffed by local government employees, without health benefits expertise, and without expertise in self-funded pooled-risk plan rate development, actuarial valuations, reserve requirements, reserve calculations, or rate-setting for a self-funded pooled-risk plan. In performance of services under this agreement, the Consultant shall at all times conform to the standard of care in the industry for a full-service health benefits consultant to a complex, self-funded client such as the SJVIA. The Consultant's conformance to that standard of care under this agreement includes, but is not limited to, the following:

(A) The Consultant shall perform as an informed, experienced, and highly educated advisor providing expert advice that is delivered in an educational, informational, competent, reliable, consistent, and objective manner.

(B) The Consultant shall conduct a review of all information and data used in calculations for rate-setting, reserving, and renewal projections, including, but not limited to, a review of employee census and enrollment data to ensure that the enrollment data used in calculations are reasonable and correctly stated. This includes, but is not limited to, a verification and comparison of SJVIA-reported cash flows and reserve levels and the information used in the experience-reporting and funding projections.

(C) A qualified health actuary shall conduct or supervise the Consultant's renewal analysis. The Consultant shall provide an actuarial report that enables the SJVIA to make well-informed decisions, including current and future funding requirements of the Insurance Programs, rate-setting, reserve types, and reserve levels.

(D) The Consultant shall provide sufficient information to allow the SJVIA to make informed decisions, including scenarios regarding the effects of the Consultant's recommendations.

(E) The Consultant shall adequately explain the risks to the SJVIA of the Consultant's proposed rates and strategies.

(F) The Consultant shall provide a clear and concise explanation of the renewal funding assumptions, including the funding effects of differing assumptions such as enrollment assumptions, trend assumptions, lag assumptions, large claim assumptions, plan design changes, and negotiated contracts.

(G) The Consultant shall provide a clear and concise explanation of limitations in the renewal data that would affect the SJVIA's decision-making, including, but not limited to, plan eligibility, enrollment, enrollment elections, turnover, cash-flow, existing reserve levels, medical and prescription drug trends, plan design changes, and large claims, as well as the effects of other internal and external drivers of costs, such as participating entities' labor negotiations and member enrollments and terminations.

1.5 **Cooperation with Management.** The Consultant shall at all times cooperate with SJVIA management, which includes the SJVIA Manager, the SJVIA Assistant Manager, the SJVIA Auditor-Treasurer, any employee of the County of Fresno or the County of Tulare who is designated by one of those persons to administer the business and activities of the SJVIA, and legal counsel to the SJVIA. That cooperation includes reporting promptly to the SJVIA Manager and the SJVIA Assistant Manager any material oral or written communications received by the Consultant from a participating entity, prospective participating entity, or contractor of the SJVIA.

1.6 **Communications to Participating Entities.** The Consultant shall provide to SJVIA management contemporaneous copies of all written communications of the Consultant on behalf of the SJVIA with any participating entity or prospective participating entity. The Consultant shall maintain written records of oral communications by the Consultant on behalf of the SJVIA to any participating entity or prospective participating entity and shall, promptly upon request by SJVIA management, provide copies of those records.

1.7 **Confidentiality.** The Consultant acknowledges that certain confidential information may be furnished by the SJVIA to the Consultant in connection with the services provided by the Consultant under this agreement ("**Confidential Information**"). The Consultant agrees that it will disclose Confidential Information only to persons who, in the Consultant's reasonable determination, need to know such information in order for the Consultant to provide services under this agreement. Disclosure by the Consultant of any Confidential Information pursuant to the terms of a valid and effective subpoena or order issued by a court of competent jurisdiction, judicial or administrative agency, or by a legislative body or committee is not a violation of this agreement. Confidential Information does not include information that:

(A) Is in the possession of the Consultant prior to its receipt of such information from the SJVIA;

(B) Is or becomes publicly available other than as a result of a breach of this agreement by the Consultant; or

(C) Is or can be independently acquired or developed by the Consultant without violating any of its obligations under this agreement.

1.8 **Compliance with Laws.** The Consultant shall, at its own cost, comply with all applicable federal, state, and local laws in performance of its services under this agreement, including but not limited to workers compensation, labor, and confidentiality laws and regulations.

Article 2
SJVIA's Obligations

2.1 **Information and Data.** Subject to the terms of this agreement, the SJVIA will provide, or authorize the vendors of its Insurance Programs to provide, the Consultant with data and information that is necessary to the Consultant's provision of services under this agreement.

2.2 **Insurance Program Premiums.** The SJVIA acknowledges that it is responsible for payment of premiums for all Insurance Programs.

Article 3
Compensation, Invoices, and Payments

3.1 **Compensation.** The SJVIA agrees to pay, and the Consultant agrees to receive, compensation for the performance of its services under this agreement as described in Exhibit B to this agreement, titled "Compensation."

3.2 **Invoices.** The Consultant shall submit monthly invoices to the SJVIA.

3.3 **Payment.** The SJVIA will pay all timely-submitted invoices within 30 days of receipt. The Consultant acknowledges that the SJVIA is a local government entity, and does so with notice that the SJVIA's powers are limited by the California Constitution and by State law, and with notice that the Consultant may receive compensation under this agreement only for

services performed according to the terms of this agreement, while this agreement is in effect, and subject to the maximum amount payable under this section. The Consultant further acknowledges that SJVIA staff have no authority to pay the Consultant except as expressly provided in this agreement.

3.4 **Incidental Expenses.** The Consultant is solely responsible for all expenses that are incidental to its performance under this agreement.

Article 4
Term and Termination

4.1 **Term.** This agreement is effective on _____ and terminates on _____. The term of this agreement may be extended for no more than two additional one-year terms by modification as provided in section 11.1 of this agreement.

4.2 **Termination for Non-Allocation of Funds.** Both parties' obligations under this agreement are contingent on the approval of funds by the appropriating government agency or agencies. If sufficient funds are not allocated, then the SJVIA, upon 30 days advance written notice to the Consultant, may:

(A) Modify either or both of the parties' obligations under this agreement; or

(B) Terminate this agreement.

4.3 **Termination for Breach; Reinstatement.**

(A) Upon determining that a breach (as defined below) has occurred, the SJVIA Manager may give written notice of the breach to the Consultant. The written notice may suspend performance under this agreement, and shall provide a reasonable time for the Consultant to cure the breach.

(B) If the Consultant fails to cure the breach within the reasonable time stated in the written notice, the SJVIA may terminate this agreement immediately.

(C) For purposes of this section, a breach occurs when the Consultant has:

(1) Obtained or used funds illegally or improperly;

(2) Failed to comply with any part of this agreement;

(3) Submitted a substantially incorrect or incomplete report to the SJVIA; or

(4) Improperly performed any of its obligations under this agreement.

4.4 **Termination for HIPAA Violation.** The SJVIA may terminate this agreement as provided in Article 8 of this agreement.

4.5 **Termination without Cause.** In circumstances other than those set forth above, the SJVIA may terminate this agreement by giving 30 days advance written notice to the Consultant.

4.6 **No Penalty or Further Obligation.** Any termination of this agreement by the SJVIA under this Article 4, or under Article 8, is without penalty to or further obligation of the SJVIA.

4.7 **SJVIA's Rights upon Termination**. Upon termination for breach under this Article 4, or under Article 8, the SJVIA may demand repayment by the Consultant of any moneys disbursed to the Consultant under this agreement that, in the SJVIA's sole judgment, were not expended in compliance with this agreement. The Consultant shall promptly refund all such monies upon demand. This section survives the expiration or termination of this agreement.

Article 5
Independent Contractor

5.1 **Status.** In performing under this agreement, the Consultant, including its officers, agents, and employees, is at all times acting and performing as an independent contractor, in an independent capacity, and not as an officer, agent, servant, employee, joint venturer, partner, or associate of the SJVIA.

5.2 **Supervision**. The SJVIA has no right to control, supervise, or direct the manner or method of the Consultant's performance under this agreement, but the SJVIA may verify that the Consultant is performing according to the terms and conditions of this agreement (for example by requesting records of communications under section 1.5 of this agreement).

5.3 **Benefits**. Because of its status as an independent contractor, the Consultant has no right to employment rights or benefits. The Consultant is solely responsible for providing to its own employees all employee benefits required by law. The Consultant shall save the SJVIA harmless from all matters relating to the payment of the Consultant's employees, including compliance with Social Security withholding and all related regulations.

5.4 **Services to Others**. The parties acknowledge that, during the term of this agreement, the Consultant may provide services to others unrelated to the SJVIA.

Article 6
Notices

6.1 **Contact Information.** The persons and their addresses having authority to give and receive notices provided for or permitted under this agreement include the following:

For the SJVIA:

SJVIA Manager
SAN JOAQUIN VALLEY INSURANCE AUTHORITY
[Street Address]
[City, State ZIP]
[Fax Number]

For the Consultant:

[Name if Desired]
[Title]
[CONSULTANT ENTITY]
[Street Address]
[City, State ZIP]
[Fax Number]

6.2 **Method of Delivery.** All notices between the SJVIA and the Consultant provided for or permitted under this agreement must be in writing and delivered either by personal service, by first-class United States mail, by an overnight commercial courier service, or by telephonic facsimile transmission.

(A) A notice delivered by personal service is effective upon service to the recipient.

(B) A notice delivered by first-class United States mail is effective three SJVIA business days after deposit in the United States mail, postage prepaid, addressed to the recipient

(C) A notice delivered by an overnight commercial courier service is effective on the SJVIA business day after deposit with the overnight commercial courier service, delivery fees prepaid, with delivery instructions given for next day delivery, addressed to the recipient.

(D) A notice delivered by telephonic facsimile is effective when transmission to the recipient is completed (but, if such transmission is completed outside of SJVIA business hours, then such delivery shall be deemed to be effective at the next beginning of a SJVIA business day), provided that the sender maintains a machine record of the completed transmission.

6.3 **Claims Presentation.** For all claims arising from or related to this agreement, nothing in this agreement establishes, waives, or modifies any claims presentation requirements or procedures provided by law, including but not limited to the Government Claims Act (Division 3.6 of Title 1 of the Government Code, beginning with section 810).

Article 7
Audits, Inspections, and Public Records

7.1 **On-Site Audits and Inspections.** The Consultant shall at any time during business hours, and as often as the SJVIA may deem necessary for any reason, make available to the SJVIA for examination all of its records and data with respect to the matters covered by this agreement.

7.2 **Document Requests.** The Consultant shall at any time, and as often as the SJVIA may deem necessary for any reason, provide copies of any records or data with respect to the matters covered by this agreement as the SJVIA may request.

7.3 **Public Records.** The SJVIA may publicly disclose this agreement under the Ralph M. Brown Act (California Government Code, Title 5, Division 2, Part 1, Chapter 9, beginning with section 54950). Except as required by Article 8 of this agreement, this agreement, and any record or data that the Consultant may provide to the SJVIA, regardless of whether it is marked as confidential or having restricted access, is subject to public disclosure as a public record under the California Public Records Act (California Government Code, Title 1, Division 7, Chapter 3.5, beginning with section 6250) ("**CPRA**").

7.4 **Public Records Act Requests.** If the SJVIA receives a written or oral request under the CPRA or a similar law to disclose any document that is in the Consultant's possession but which the SJVIA has a right to possessor control, then the SJVIA may demand, in writing, that the Consultant deliver to the SJVIA, for purposes of public disclosure, the requested records that may be in the possession or control of the Consultant. Within five business days after the SJVIA's demand, the Consultant shall (a) deliver to the SJVIA all of the requested records that are in the Consultant's possession or control, together with a written statement that the Consultant has produced all requested records that are in the Consultant's possession or control, or (b) provide to the SJVIA a written statement that the Consultant does not possess or control any of the requested records. The Consultant shall cooperate with the SJVIA with respect to any SJVIA demand for such records. The Consultant shall indemnify the SJVIA for any award of costs or attorney's fees under the CPRA that results from the Consultant's delay, claim of exemption, failure to produce such records, or failure to cooperate with the SJVIA with respect to any SJVIA demand for such records.

7.5 **State Audit Requirements.** If this agreement exceeds $10,000, the Consultant is subject to the examination and audit of the California State Auditor, as provided in Government Code section 8546.7, for a period of three years after final payment under this agreement. The obligations under this section survive the termination of this agreement.

7.6 **Ownership of Records.**

(A) Upon the performance of services under this agreement by the Consultant and payment by the SJVIA to the Consultant for those services, every written or electronic writing, document, data, tables, analysis, or reports, including, but not limited to, all insurance documents, insurance policies, memoranda of coverage, certificates of coverage, endorsements to coverage, claims reports and records, loss reports, financial records and statements, claims management agreements and audits, program promotional materials and correspondence between the Consultant and the SJVIA, its participating entities, or both, that is generated as a result of the Consultant's performance of services under this agreement shall remain the exclusive property of the SJVIA. The consultant shall be entitled to keep a copy of such files and documents as may be necessary to demonstrate its performance under this agreement.

(B) In the event of termination or cancellation of this agreement, the Consultant shall return all such records and files to the SJVIA unless the SJVIA requests the Consultant to process any work or file in progress, which the Consultant will continue to process on a time and expense basis or as mutually agreed by the parties in writing. When such

work is completed, all records and files relating to the work shall be returned to the SJVIA.

Article 8
Health Insurance Portability and Accountability Act

8.1 The parties to this agreement shall be in strict conformance with all applicable federal and State of California laws and regulations, including but not limited to: Sections 5328, 10850, and 14100.2 et seq. of the California Welfare and Institutions Code; Sections 2.1 and 431.300 et seq. of Title 42, Code of Federal Regulations ("**CFR**"); Section 56 et seq. of the California Civil Code; Sections 11977 and 11812 of Title 22 of the California Code of Regulations; the Health Insurance Portability and Accountability Act, as amended, including but not limited to Section 1320 D et seq. of Title 42, United States Code, and its implementing regulations, including but not limited to Title 45, CFR, Parts 142, 160, 162, and 164 (collectively, "**HIPAA**"); the Health Information Technology for Economic and Clinical health Act, as amended ("**HITECH**"), regarding the confidentiality and security of patient information; and the Genetic Information Nondiscrimination Act of 2008, as amended ("**GINA**"), regarding the confidentiality of genetic information.

8.2 Except as otherwise provided in this agreement, the Consultant, as a business associate of the SJVIA, may use or disclose Protected Health Information ("**PHI**") to perform functions, activities, or services for or on behalf of the SJVIA, as specified in this agreement provided that such use or disclosure does not violate HIPAA. The uses and disclosures of PHI may not be more expansive than those applicable to SJVIA, as the covered entity under the HIPAA Privacy Rule (45 CFR § 164.500 et seq.), except as authorized for management, administrative, or legal responsibilities of the business associate.

8.3 The Consultant, including its authorized subcontractors and employees, shall protect from unauthorized access, use, or disclosure the names and other identifying information, including genetic information, concerning persons receiving services under the Insurance Programs, except where permitted in order to carry out data aggregation for purposes of health care operations (45 CFR §§ 164.504(e)(2)(i), 164.504(e)(2)(ii)(A), and 164.504(e)(4)(i)). This requirement applies to electronic PHI. The Consultant shall not use such identifying information or genetic information for any purpose other than carrying out the Consultant's obligations under this agreement.

8.4 The consultant, including its authorized subcontractors and employees, shall not disclose any such identifying information or genetic information to any person or entity, except as otherwise specifically permitted by this agreement, authorized by Subpart E of 45 CFR Part 164 or other law, required by the Secretary, or authorized by the client or patient in writing. In using or disclosing PHI that is permitted by this agreement or authorized by law, the Consultant shall make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

8.5 For the purposes of the above sections, identifying information includes, but is not limited to, name, identifying number, symbol, or other identifying particular assigned to an individual, such as a finger- or voiceprint, or photograph.

8.6 For purposes of the above sections, genetic information includes, but is not limited to, genetic tests of an individual or family members of the individual, manifestation of disease or disorder of an individual or family members of the individual, or any request for or receipt of genetic services by an individual or family members of the individual. Family member means a dependent or any person who is a first, second, third, or fourth degree relative.

8.7 At the request of the SJVIA, and in the time and manner specified by the SJVIA, the Consultant shall provide, to the SJVIA or to an individual, PHI in a designated record set (as defined in 45 CFR § 164.501) in order to meet the requirements of 45 CFR § 164.524 regarding access by individuals to their PHI. With respect to individual requests, the Consultant shall provide access within 30 days of the request. That deadline may be extended if the Contractor cannot provide access and provides the reasons for the delay and the reasonable date when access may be granted. The consultant shall provide PHI in the form and format requested by the SJVIA or the individual.

8.8 The Consultant shall make amendment or amendments to PHI in a designated record set in accordance with 45 CFR § 164.526.

8.9 The Consultant shall provide to the SJVIA or to an individual, in the time and manner specified by the SJVIA, information collected in accordance with 45 CFR § 164.528, to permit the SJVIA to respond to a request by the individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

8.10 The Consultant shall, immediately and without unreasonable delay and in no case later than two business days after discovery, report to the SJVIA's Privacy Officer, in writing, any knowledge or reasonable belief that there has been unauthorized access, viewing, use, disclosure, security incident, or breach of unsecured PHI not permitted by this agreement of which it becomes aware. The notification shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, disclosed, or breached. The Consultant shall take prompt corrective action to cure any deficiencies and any action pertaining to such unauthorized disclosure required by applicable federal and State of California laws and regulations. The Consultant shall investigate such breach and is responsible for all notifications required by law, regulation, or both, or deemed necessary by the SJVIA, and shall provide a written report of the investigation and reporting required to the SJVIA's Privacy Officer. This written investigation and description of any reporting necessary shall be postmarked as mailed to the SJVIA's Privacy Officer within 30 working days of the discovery of the breach.

8.11 The Consultant shall make its internal practices, books, and records relating to the use and disclosure of PHI received from SJVIA, or created or received by the Consultant on behalf of the SJVIA, in compliance with the HIPAA Privacy Rule, including but not limited to the requirements set forth in 45 CFR Parts 160 and 164. The Consultant shall make its internal

practices, books, and records relating to the use and disclosure of PHI received from the SJVIA, or created or received by the Consultant on behalf of the SJVIA, available to the United States Department of Health and Human Services upon demand.

8.12 The Consultant shall cooperate with the compliance and investigation reviews conducted by the Secretary. The Consultant must provide PHI access to the Secretary during the Consultant's normal business hours, but upon exigent circumstances shall also grant access at any time. Upon the Secretary's compliance or investigation review, if PHI is unavailable to the Consultant and in possession of a subcontractor, the Consultant must certify to the Secretary its efforts to obtain the information.

8.13 **Safeguards.** The Consultant shall implement administrative, physical, and technical safeguards as required by the HIPAA Security Rule, Subpart C of 45 CFR Part 164, that reasonably and appropriately protects the confidentiality, integrity, and availability of PHI, including electronic PHI, that it creates, receives, maintains or transmits on behalf of the SJIVA and to prevent unauthorized access, viewing, use, disclosure, or breach of PHI other than as provided for by this agreement. The Consultant shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidential, integrity and availability of electronic PHI. The Consultant 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 Consultant's operations and the nature and scope of its activities. Upon the SJVIA's request, the Consultant shall provide the SJVIA with information concerning such safeguards.

8.14 **Security Safeguards and Precautions.** The Consultant shall implement strong access controls and other security safeguards and precautions in order to restrict logical and physical access to confidential, personal (e.g., PHI) or sensitive data to authorized users only.

8.15 **Password Controls.** Those safeguards and precautions shall include the following administrative and technical password controls for all systems used to process or store confidential, personal, or sensitive data.

(A) Passwords must not be:

(1) Shared or written down where they are accessible or recognizable by anyone else; such as taped to computer screens, stored under keyboards, or visible in a work area;

(2) A dictionary word; or

(3) Stored in clear text

(B) Passwords must be:

(1) Eight characters or more in length;

(2) Changed every 90 days;

(3) Changed immediately if revealed or compromised; and

(4) Composed of characters from at least three of the following four groups from the standard keyboard: (i) upper case letters (A-Z); (ii) lowercase letters (a-z); (iii) Arabic numerals (0 through 9); and (iv) non-alphanumeric characters (punctuation symbols).

8.16 **Security Controls.** The Consultant shall implement the following security controls on each workstation or portable computing device (e.g., laptop computer) containing confidential, personal, or sensitive data:

(A) Network-based firewall and/or personal firewall;

(B) Continuously updated anti-virus software; and

(C) Patch management process including installation of all operating system/software vendor security patches.

8.17 **Encryption.** The Consultant shall us a commercial encryption solution that has received FIPS 140-2 validation to encrypt all confidential, personal, or sensitive data stored on portable electronic media (including, but not limited to, compact disks and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers).

8.18 **Data Transmission.** The Consultant shall not transmit confidential, personal, or sensitive data via e-mail or other internet transport protocol unless the data is encrypted by a solution that has been validated by the National Institute of Standards and Technology (NIST) as conforming to the Advanced Encryption Standard (AES) Algorithm. The Consultant must apply appropriate sanctions against its employees who fail to comply with these safeguards. The Consultant must adopt procedures for terminating access to PHI when employment of employee ends.

8.19 **Mitigation of Harmful Effects.** The Consultant shall mitigate, to the extent practicable, any harmful effect that is suspected or known to the Consultant of an unauthorized access, viewing, use, disclosure, or breach of PHI by the Consultant or its subcontractors in violation of the requirements of this Article 8. The Consultant must document suspected or known harmful effects and the outcome of any mitigation.

8.20 **Consultant's Subcontractors.** The Consultant shall ensure that each of its contractors, including subcontractors, if applicable, to whom the Consultant provides PHI received from or created or received by the Consultant from or on behalf of the SJVIA, agrees to the same restrictions, safeguards, and conditions that apply to the Consultant with respect to such PHI and to incorporate, when applicable, the relevant provisions of these provisions into each subcontract or sub-award to such agents or subcontractors.

8.21 **Employee Training and Discipline.** The Consultant shall train and use reasonable measures to ensure compliance with the requirements of the provisions of this Article 8 by employees who assist in the performance of functions or activities on behalf of the SJVIA under

this agreement and use or disclose PHI and discipline such employees who intentionally violate any provisions of these provisions, including termination of employment.

8.22 **Termination for Breach.** Upon the SJVIA's knowledge of a material breach of these provisions by the Consultant, the SJVIA shall either:

(A) Provide an opportunity for the Consultant to cure the breach or end the violation, and the terminate this agreement if the Consultant does not cure the breach or end the violation within the time specified by the SJVIA; or

(B) Immediately terminate this agreement if the Consultant has breached a material term of these provisions and cure is not possible.

(C) If neither cure nor termination is feasible, the SJVIA's Privacy Officer shall report the violation to the Secretary.

8.23 **Termination after Judicial or Administrative Proceedings.** The SJVIA may terminate this agreement if: (1) the Consultant is found guilty in a criminal proceeding for a violation of the HIPAA Privacy or Security Laws or the HITECH Act; or (2) there is a finding or stipulation that the Consultant has violated a privacy or security standard or requirement of the HITECH Act, HIPAA, or other security or privacy laws in an administrative or civil proceeding in which the Consultant is a party.

8.24 **Obligations upon Termination.** Upon termination or expiration of this agreement for any reason, the Consultant shall return or destroy all PHI received from the SJVIA (or created or received by the Consultant on behalf of SJVIA) that the Consultant still maintains in any form, and shall retain no copies of such PHI. If return or destruction of PHI is not feasible, the Consultant shall continue to extend the protections of these provisions to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision applies to PHI that is in the possession of subcontractors or agents, if applicable, of the Consultant. If the Consultant destroys the PHI data, the Consultant shall provide to the SJVIA a certification of date and time of destruction

8.25 **Disclaimer.** The SJVIA makes no warranty or representation that compliance by the Consultant with the provisions of this Article 8, HIPAA, or HITECH will be adequate or satisfactory for the Consultant's own purposes or that any information in the Consultant's possession or control, or transmitted or received by the Consultant, is or will be secure from unauthorized access, viewing, use, disclosure, or breach. The Consultant is solely responsible for all decisions made by the Consultant regarding the safeguarding of PHI.

8.26 **Amendment.** The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of these provisions may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to amend this agreement in order to implement the standards and requirements of HIPAA, HITECH, and other applicable laws relating to the security or privacy of PHI. The SJVIA may terminate this agreement upon 30 days written notice if the Consultant does not enter into an amendment

providing assurances regarding the safeguarding of PHI that the SJVIA in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and HITECH.

8.27 **Interpretation.** The terms of this Article 8 shall be interpreted as broadly as necessary to implement and comply with HIPAA and applicable State of California laws. The parties agree that any ambiguity in the terms and conditions of these provisions shall be resolved in favor of a meaning that complies and is consistent with HlPAA.

8.28 **Regulatory References.** Any reference in this agreement to a law or regulation means the law or regulation as in effect or as amended.

8.29 **Survival.** The obligations of the Consultant as provided in this Article 8 survive the termination or expiration of this agreement.

8.30 **Definitions.** For purposes of this Article 8:

(A) The SJVIA's Privacy Officer is the SJVIA Manager.

(B) The Secretary is as defined in 45 CFR § 160.103

Article 9
Indemnity

9.1 **Indemnification.** The Consultant shall indemnify and defend the SJVIA (including its officers, agents, employees, and volunteers) against all claims, demands, injuries, damages, costs, expenses (including attorney fees and costs), fines, penalties, and liabilities of any kind to the SJVIA, the Consultant, or any third party that arise from or relate to the performance or failure to perform by the Consultant (or any of its officers, agents, or employees) under this agreement. The SJVIA may conduct or participate in its own defense without affecting the Consultant's obligation to indemnify or defend the SJVIA.

9.2 **Limitation.** The indemnity required by this agreement, including section 9.1, is not intended, and shall not be construed, to exceed the limitations in California Civil Code sections 2782 through 2784.5.

9.3 **Survival**. This Article 9 survives the expiration or termination of this agreement.

Article 10
Data Security

10.1 **Definitions.** Capitalized terms used in this agreement have the meanings set forth in this section 10.1:

(A) "**Authorized Employees**" means the Consultant's employees who have access to Personal Information.

(B) "**Authorized Persons**" means: (i) any and all Authorized Employees; and (ii) any and all of the Consultant's subcontractors, representatives, agents, outsourcers, and consultants, and providers of professional services to the Consultant, who have access

to Personal Information and are bound by law or in writing by confidentiality obligations sufficient to protect Personal Information in accordance with the terms of this Article 10.

(C) "**Disclose**" or any derivative of that word means to disclose, release, transfer, disseminate, or otherwise provide access to or communicate all or any part of any Personal Information orally, in writing, or by electronic or any other means to any person.

(D) "**Manager**" means the SJVIA Manager or the SJVIA Assistant Manager.

(E) "**Person**" means any natural person, corporation, partnership, limited liability company, firm, or association.

(F) "**Personal Information**" means any and all information, including any data, provided, or to which access is provided, to the Consultant by or upon the authorization of the SJVIA, under this Agreement, including but not limited to vital records, that: (i) identifies, describes, or relates to, or is associated with, or is capable of being used to identify, describe, or relate to, or associate with, a person (including, without limitation, names, physical descriptions, signatures, addresses, telephone numbers, e-mail addresses, education, financial matters, employment history, and other unique identifiers, as well as statements made by or attributable to the person); (ii) is used or is capable of being used to authenticate a person (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or personal identification numbers (PINs), financial account numbers, credit report information, answers to security questions, and other personal identifiers); or (iii) is personal information within the meaning of California Civil Code section 1798.3, subdivision (a), or 1798.80, subdivision (e). Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(G) "**Privacy Practices Complaint**" means a complaint received by the SJVIA relating to the Consultant's (or any Authorized Person's) privacy practices, or alleging a Security Breach. Such complaint shall have sufficient detail to enable the SJVIA to promptly investigate and take remedial action under this Article 10.

(H) "**Security Breach**" means (i) any act or omission that compromises either the security, confidentiality, value, or integrity of any Personal Information or the Security Safeguards, or (ii) any unauthorized Use, Disclosure, or modification of, or any loss or destruction of, or any corruption of or damage to, any Personal Information.

(I) "**Security Safeguards**" means physical, technical, administrative or organizational security procedures and practices put in place by the Consultant (or any Authorized Persons) that relate to the protection of the security, confidentiality, value, or integrity of Personal Information. Security Safeguards shall satisfy the minimal requirements set forth in section 10.3(C) of this agreement.

(J) "**Use**" or any derivative thereof means to receive, acquire, collect, apply, manipulate, employ, process, transmit, disseminate, access, store, disclose, or dispose of Personal Information.

10.2 **Standard of Care.**

(A) The Consultant acknowledges that, in the course of its engagement by the SJVIA under this agreement, the Contractor, or any Authorized Persons, may Use Personal Information only as permitted in this agreement.

(B) The Consultant acknowledges that Personal Information is deemed to be confidential information of, or owned by, the SJVIA (or persons from whom the SJVIA receives or has received Personal Information) and is not confidential information of, or owned or by, the Consultant, or any Authorized Persons. The Consultant further acknowledges that all right, title, and interest in or to the Personal Information remains in the SJVIA (or persons from whom the SJVIA receives or has received Personal Information) regardless of the Consultant's, or any Authorized Person's, Use of that Personal Information.

(C) The Consultant agrees and covenants in favor of the SJVIA that the Consultant shall:

(1) keep and maintain all Personal Information in strict confidence, using such degree of care under this section 10.2 as is reasonable and appropriate to avoid a Security Breach;

(2) Use Personal Information exclusively for the purposes for which the Personal Information is made accessible to the Consultant pursuant to the terms of this Article 10;

(3) not Use, Disclose, sell, rent, license, or otherwise make available Personal Information for the Consultant's own purposes or for the benefit of anyone other than the SJVIA, without the SJVIA's express prior written consent, which the SJVIA may give or withhold in its sole and absolute discretion; and

(4) not, directly or indirectly, Disclose Personal Information to any person (an "**Unauthorized Third Party**") other than Authorized Persons pursuant to this Agreement, without the Manager's express prior written consent.

(D) Notwithstanding the foregoing paragraph, in any case in which the Consultant believes it, or any Authorized Person, is required to disclose Personal Information to government regulatory authorities, or pursuant to a legal proceeding, or otherwise as may be required by applicable law, Consultant shall (i) immediately notify the SJVIA of the specific demand for, and legal authority for the disclosure, including providing the SJVIA with a copy of any notice, discovery demand, subpoena, or order, as applicable, received by the Consultant, or any Authorized Person, from any government regulatory authorities, or in relation to any legal proceeding, and (ii) promptly notify the SJVIA before such Personal Information is offered by the Consultant for such disclosure so that

the SJVIA may have sufficient time to obtain a court order or take any other action the SJVIA may deem necessary to protect the Personal Information from such disclosure, and the Consultant shall cooperate with the SJVIA to minimize the scope of such disclosure of such Personal Information.

(E) The Consultant shall remain liable to the SJVIA for the actions and omissions of any Unauthorized Third Party concerning its Use of such Personal Information as if they were the Consultant's own actions and omissions.

10.3 **Information Security**.

(A) The Consultant covenants, represents and warrants to the SJVIA that the Consultant's Use of Personal Information under this Agreement does and will at all times comply with all applicable federal, state, and local, privacy and data protection laws, as well as all other applicable regulations and directives, including but not limited to California Civil Code, Division 3, Part 4, Title 1.81 (beginning with section 1798.80), and the Song-Beverly Credit Card Act of 1971 (California Civil Code, Division 3, Part 4, Title 1.3, beginning with section 1747). If the Consultant Uses credit, debit or other payment cardholder information, the Consultant shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing and maintaining all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the Consultant's sole cost and expense.

(B) The Consultant covenants, represents and warrants to the SJVIA that, as of the effective date of this agreement, the Consultant has not received notice of any violation of any privacy or data protection laws, as well as any other applicable regulations or directives, and is not the subject of any pending legal action or investigation by, any government regulatory authority regarding same.

(C) Without limiting the Consultant's obligations under section 10.3(A) of this agreement, the Consultant's (or Authorized Person's) Security Safeguards shall be no less rigorous than accepted industry practices and, at a minimum, include the following:

(1) limiting Use of Personal Information strictly to the Consultant's and Authorized Persons' technical and administrative personnel who are necessary for the Consultant's, or Authorized Persons', Use of the Personal Information pursuant to this agreement;

(2) ensuring that all of the Consultant's connectivity to SJVIA computing systems will only be through the SJVIA's security gateways and firewalls, and only through security procedures approved upon the express prior written consent of the Manager;

(3) to the extent that they contain or provide access to Personal Information, (a) securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, operating systems, and software applications, including, but not limited to, all mobile devices and other equipment, operating systems, and software

applications with information storage capability; (b) employing adequate controls and data security measures, both internally and externally, to protect (1) the Personal Information from potential loss or misappropriation, or unauthorized Use, and (2) the SJVIA's operations from disruption and abuse; (c) having and maintaining network, device application, database and platform security; (d) maintaining authentication and access controls within media, computing equipment, operating systems, and software applications; and (e) installing and maintaining in all mobile, wireless, or handheld devices a secure internet connection, having continuously updated anti-virus software protection and a remote wipe feature always enabled, all of which is subject to express prior written consent of the Manager;

(4) encrypting all Personal Information at advance encryption standards of Advanced Encryption Standards (AES) of 128 bit or higher (a) stored on any mobile devices, including but not limited to hard disks, portable storage devices, or remote installation, or (b) transmitted over public or wireless networks (the encrypted Personal Information must be subject to password or pass phrase, and be stored on a secure server and transferred by means of a Virtual Private Network (VPN) connection, or another type of secure connection, all of which is subject to express prior written consent of the Manager);

(5) strictly segregating Personal Information from all other information of the Consultant, including any Authorized Person, or anyone with whom the Consultant or any Authorized Person deals so that Personal Information is not commingled with any other types of information;

(6) having a patch management process including installation of all operating system and software vendor security patches;

(7) maintaining appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks of Authorized Employees consistent with applicable law; and

(8) providing appropriate privacy and information security training to Authorized Employees.

(D) During the term of each Authorized Employee's employment by the Consultant, the Consultant shall cause such Authorized Employees to abide strictly by the Contractor's obligations under this Article 10. The Consultant shall maintain a disciplinary process to address any unauthorized Use of Personal Information by any Authorized Employees.

(E) The Consultant shall, in a secure manner, backup daily, or more frequently if it is the Consultant's practice to do so more frequently, Personal Information received from the SJVIA, and the SJVIA shall have immediate, real time access, at all times, to such backups via a secure, remote access connection provided by the Consultant, through the Internet.

(F) The Consultant shall provide the SJVIA with the name and contact information for each Authorized Employee (including such Authorized Employee's work shift, and at least one alternate Authorized Employee for each Authorized Employee during such work shift) who shall serve as the SJVIA's primary security contact with the Consultant and shall be available to assist the SJVIA twenty-four (24) hours per day, seven (7) days per week as a contact in resolving the Consultant's and any Authorized Persons' obligations associated with a Security Breach or a Privacy Practices Complaint.

(G) The Consultant shall not knowingly include or authorize any Trojan Horse, back door, time bomb, drop dead device, worm, virus, or other code of any kind that may disable, erase, display any unauthorized message or otherwise impair SJVIA computing systems, with or without the intent to cause harm.

10.4 **Security Breach Procedures.**

(A) Immediately upon the Consultant's awareness or reasonable belief of a Security Breach, the Contractor shall (i) notify the Manager of the Security Breach, such notice to be given first by telephone at the following telephone number, followed promptly by email at the following email address: (559) 600-1810 / SJVIA-Admin@fresnocountyca.gov (which telephone number and email address the SJVIA may update by providing notice to the Consultant), and (ii) preserve all relevant evidence (and cause any affected Authorized Person to preserve all relevant evidence) relating to the Security Breach. The notification shall include, to the extent reasonably possible, the identification of each type and the extent of Personal Information that has been, or is reasonably believed to have been, breached, including but not limited to, compromised, or subjected to unauthorized Use, Disclosure, or modification, or any loss or destruction, corruption, or damage.

(B) Immediately following the Consultant's notification to the SJVIA of a Security Breach, as provided pursuant to section 10.4(A) of this agreement, the parties shall coordinate with each other to investigate the Security Breach. The Consultant agrees to fully cooperate with the SJVIA, including, without limitation:

(1) assisting the SJVIA in conducting any investigation;

(2) providing the SJVIA with physical access to the facilities and operations affected;

(3) facilitating interviews with Authorized Persons and any of the Consultant's other employees knowledgeable of the matter; and

(4) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by the SJVIA.

To that end, the Consultant shall, with respect to a Security Breach, be solely responsible, at its cost, for all notifications required by law and regulation, or deemed

reasonably necessary by the SJVIA, and the Consultant shall provide a written report of the investigation and reporting required to the Manager within 30 days after the Consultant's discovery of the Security Breach.

(C) The SJVIA shall promptly notify the Consultant of the Manager's knowledge, or reasonable belief, of any Privacy Practices Complaint, and upon the Consultant's receipt of notification thereof, the Consultant shall promptly address such Privacy Practices Complaint, including taking any corrective action under this Article 10, all at the Consultant's sole expense, in accordance with applicable privacy rights, laws, regulations and standards. If the Consultant discovers a Security Breach, the Consultant shall treat the Privacy Practices Complaint as a Security Breach. Within 24 hours of the Consultant's receipt of notification of such Privacy Practices Complaint, the Consultant shall notify the SJVIA whether the matter is a Security Breach, or otherwise has been corrected and the manner of correction, or determined not to require corrective action and the reason therefor.

(D) The Consultant shall take prompt corrective action to respond to and remedy any Security Breach and take mitigating actions, including but not limiting to, preventing any reoccurrence of the Security Breach and correcting any deficiency in Security Safeguards as a result of such incident, all at the Consultant's sole expense, in accordance with applicable privacy rights, laws, regulations and standards. The Consultant shall reimburse the SJVIA for all reasonable costs incurred by the SJVIA in responding to, and mitigating damages caused by, any Security Breach, including all costs of the SJVIA incurred relation to any litigation or other action described section 10.4(E) of this agreement.

(E) The Consultant agrees to cooperate, at its sole expense, with the SJVIA in any litigation or other action to protect the SJVIA's rights relating to Personal Information, including the rights of persons from whom the SJVIA receives Personal Information.

10.5 **Oversight of Security Compliance.**

(A) The Consultant shall have and maintain a written information security policy that specifies Security Safeguards appropriate to the size and complexity of the Consultant's operations and the nature and scope of its activities.

(B) Upon the SJVIA's written request, to confirm the Consultant's compliance with this Article 10, as well as any applicable laws, regulations and industry standards, the Consultant grants the SJVIA or, upon the SJVIA's election, a third party on the SJVIA's behalf, permission to perform an assessment, audit, examination or review of all controls in the Consultant's physical and technical environment in relation to all Personal Information that is Used by the Consultant pursuant to this agreement. The Consultant shall fully cooperate with such assessment, audit or examination, as applicable, by providing the SJVIA or the third party on the SJVIA's behalf, access to all Authorized Employees and other knowledgeable personnel, physical premises, documentation, infrastructure and application software that is Used by the Consultant for Personal

Information pursuant to this agreement. In addition, the Consultant shall provide the SJVIA with the results of any audit by or on behalf of the Consultant that assesses the effectiveness of the Consultant's information security program as relevant to the security and confidentiality of Personal Information Used by the Consultant or Authorized Persons during the course of this agreement under this Article 10.

(C) The Consultant shall ensure that all Authorized Persons who Use Personal Information agree to the same restrictions and conditions in this Article 10 that apply to the Consultant with respect to such Personal Information by incorporating the relevant provisions of these provisions into a valid and binding written agreement between the Consultant and such Authorized Persons, or amending any written agreements to provide same.

10.6 **Return or Destruction of Personal Information.** Upon the expiration or termination of this agreement, the Consultant shall, and shall instruct all Authorized Persons to, promptly return to the SJVIA all Personal Information, whether in written, electronic or other form or media, in its possession or the possession of such Authorized Persons, in a machine readable form used by the SJVIA at the time of such return, or upon the express prior written consent of the Manager, securely destroy all such Personal Information, and certify in writing to the the SJVIA that such Personal Information have been returned to the SJVIA or disposed of securely, as applicable. If the Consultant is authorized to dispose of any such Personal Information, as provided in this Article 10, such certification shall state the date, time, and manner (including standard) of disposal and by whom, specifying the title of the individual. The Consultant shall comply with all reasonable directions provided by the Manager with respect to the return or disposal of Personal Information and copies thereof. If return or disposal of such Personal Information or copies of Personal Information is not feasible, the Consultant shall notify the SJVIA accordingly, specifying the reason, and continue to extend the protections of this Article 10 to all such Personal Information and copies of Personal Information. The Consultant shall not retain any copy of any Personal Information after returning or disposing of Personal Information as required by this section 10.6. The Consultant's obligations under this section 10.6 survive the expiration or termination of this agreement and apply to all Personal Information that the Consultant retains if return or disposal is not feasible and to all Personal Information that the Consultant may later discover.

10.7 **Equitable Relief.** The Consultant acknowledges that any breach of its covenants or obligations set forth in this Article 10 may cause the SJVIA irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the SJVIA is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the SJVIA may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available to the SJVIA at law or in equity or under this agreement.

10.8 **Indemnity.** The Consultant shall defend, indemnify and hold harmless the SJVIA, its officers, employees, and agents, (each, an **"SJVIA Indemnitee"**) from and against any and all

infringement of intellectual property including, but not limited to infringement of copyright, trademark, and trade dress, invasion of privacy, information theft, and extortion, unauthorized Use, Disclosure, or modification of, or any loss or destruction of, or any corruption of or damage to, Personal Information, Security Breach response and remedy costs, credit monitoring expenses, forfeitures, losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, fines and penalties (including regulatory fines and penalties), costs or expenses of whatever kind, including attorneys' fees and costs, the cost of enforcing any right to indemnification or defense under this Article 10 and the cost of pursuing any insurance providers, arising out of or resulting from any third party claim or action against any SJVIA Indemnitee in relation to the Consultant's, its officers, employees, or agents, or any Authorized Employee's or Authorized Person's, performance or failure to perform under this Article 10 or arising out of or resulting from the Consultant's failure to comply with any of its obligations under this section 10.8. The provisions of this section 10.8 do not apply to the acts or omissions of the SJVIA. The provisions of this section 10.8 are cumulative to any other obligation of the SJVIA to, defend, indemnify, or hold harmless any SJVIA Indemnitee under this agreement. The provisions of this section 10.8 shall survive the expiration or termination of this agreement.

10.9 **Survival.** The respective rights and obligations of the Consultant and the SJVIA as stated in this Article 10 shall survive the expiration or termination of this agreement.

10.10 **No SJVIA Warranty.** The SJVIA does not make any warranty or representation whether any Personal Information in the Consultant's (or any Authorized Person's) possession or control, or Use by the Consultant (or any Authorized Person), pursuant to the terms of this agreement is or will be secure from unauthorized Use, or a Security Breach or Privacy Practices Complaint.

Article 11
Insurance

11.1 **Policy and Coverage Requirements.** Without limiting the SJVIA's right to obtain indemnification from the Consultant or any third parties, the Consultant, at its sole expense, shall maintain in full force and effect, the following insurance policies throughout the term of this agreement.

(A) **Commercial General Liability.** Commercial general liability insurance with limits of not less than Two Million Dollars ($2,000,000) per occurrence and an annual aggregate of Four Million Dollars ($4,000,000). The Consultant shall obtain an endorsement to this policy naming the SJVIA, its officers, agents, employees, and volunteers, individually and collectively, as additional insureds, but only insofar as the operations under this agreement are concerned. Such coverage for additional insureds will apply as primary insurance and any other insurance, or self-insurance, maintained by the SJVIA is excess only and not contributing with insurance provided under the Consultant's policy.

(B) **Automobile Liability.** Automobile liability insurance with limits of not less than One Million Dollars ($1,000,000) per occurrence for bodily injury and for property damages. Coverage must include any auto used in connection with this Agreement.

(C) **Professional Liability.** Professional liability insurance with limits of not less than One Million Dollars ($1,000,000) per occurrence and an annual aggregate of Three Million Dollars ($3,000,000). If this is a claims-made policy, then (1) the retroactive date must be prior to the date on which services began under this Agreement; (2) the Consultant shall maintain the policy and provide to the SJVIA annual evidence of insurance for not less than five years after completion of services under this agreement; and (3) if the policy is canceled or not renewed, and not replaced with another claims-made policy with a retroactive date prior to the date on which services begin under this agreement, then the Consultant shall purchase extended reporting coverage on its claims-made policy for a minimum of five years after completion of services under this agreement.

(D) **Workers Compensation.** Workers compensation insurance as required by the California Labor Code.

(E) **Cyber Liability.** Cyber liability insurance with limits of not less than Two Million Dollars ($2,000,000) per occurrence. Coverage must include, but not be limited to, claims involving Cyber Risks. The cyber liability policy must be endorsed to cover the full replacement value of damage to, alteration of, loss of, or destruction of intangible property (including but not limited to information or data) that is in the care, custody, or control of the Consultant.

Definition of Cyber Risks. "Cyber Risks" include but are not limited to (i) Security Breaches, which may include Disclosure of Personal Information to an Unauthorized Third Party; (ii) breach of any of the Contractor's obligations under Article 10 of this Agreement; (iii) infringement of intellectual property, including but not limited to infringement of copyright, trademark, and trade dress; (iv) invasion of privacy, including release of private information; (v) information theft; (vi) damage to or destruction or alteration of electronic information; (vii) extortion related to the Contractor's obligations under this Agreement regarding electronic information, including Personal Information; (viii) network security; (ix) data breach response costs, including Security Breach response costs; (x) regulatory fines and penalties related to the Contractor's obligations under this Agreement regarding electronic information, including Personal Information; and (xi) credit monitoring expenses.

11.2 **Verification of Coverage.** Within 30 days after the Consultant signs this agreement, the Consultant shall deliver, or cause its broker or producer to deliver, to SJVIA Administration, at 2220 Tulare Street, Suite 1400, Fresno, California 93721, or SJVIA-Admin@fresnocountyca.gov, copies of insurance policies as produced by the broker or producer, and certificates of insurance and endorsements for all of the coverages required under this agreement.

(A) All insurance certificates must state that: (1) the insurance coverage has been obtained and is in full force; (2) the SJVIA, its officers, agents, employees, and volunteers are not responsible for any premiums on the policy; and (3) the Consultant has waived its right to recover from the SJVIA, its officers, agents, employees, and volunteers any amounts paid under any insurance policy required by this agreement and that waiver does not invalidate the insurance policy.

(B) The commercial general liability insurance certificate must also state that: (1) the SJVIA, its officers, agents, employees, and volunteers, individually and collectively, are additional insureds insofar as the operations under this agreement are concerned; (2) the coverage shall apply as primary insurance and any other insurance, or self-insurance, maintained by the SJVIA shall be excess only and not contributing with insurance provided under the Consultant's policy.

(C) The automobile liability insurance certificate must state that the policy covers any auto used in connection with this agreement.

(D) The professional liability insurance certificate, if it is a claims-made policy, must also state the retroactive date of the policy, which must be prior to the date on which services began under this agreement.

(E) The cyber liability insurance certificate must also state that it is endorsed to cover the full replacement value of damage to, alteration of, loss of, or destruction of intangible property (including but not limited to information or data) that is in the care, custody, or control of the Consultant.

11.3 **Acceptability of Insurers.** All insurance policies required under this agreement must be issued by admitted insurers licensed to do business in the State of California and possessing at all times during the term of this agreement an A.M. Best, Inc. rating of A:VII or greater.

11.4 **Notice of Cancellation or Change.** For each insurance policy required under this agreement, the Consultant shall provide to the SJVIA, or ensure that the policy requires the insurer to provide to the SJVIA, written notice of any cancellation or change in the policy as required in this paragraph. For cancellation of the policy for nonpayment of premium, the Consultant shall, or shall cause the insurer to, provide written notice to the SJVIA not less than 10 days in advance of cancellation. For cancellation of the policy for any other reason, and for any other change to the policy, the Consultant shall, or shall cause the insurer to, provide written notice to the SJVIA not less than 30 days in advance of cancellation or change. The SJVIA in its sole discretion may determine that the failure of the Consultant or its insurer to timely provide a written notice required by this paragraph is a breach of this agreement.

11.5 **SJVIA's Entitlement to Greater Coverage.** If the Consultant has or obtains insurance with broader coverage, higher limits, or both, than what is required under this agreement, then the SJVIA requires and is entitled to the broader coverage, higher limits, or both. To that end, the Consultant shall deliver, or cause its broker or producer to deliver, to

SJVIA Administration copies of insurance policies that have such broader coverage, higher limits, or both, as produced by the broker or producer, and certificates of insurance and endorsements for all of the coverages that have such broader coverage, higher limits, or both, as required under this agreement.

11.6 **Waiver of Subrogation.** The Consultant waives its right to recover from the SJVIA, its officers, agents, employees, and volunteers any amounts paid under the policy of worker's compensation insurance required by this agreement. The Consultant is solely responsible to obtain any policy endorsement that may be necessary to accomplish that waiver, but the Consultant's waiver of subrogation under this paragraph is effective whether or not the Consultant obtains such an endorsement.

11.7 **SJVIA's Remedy for Consultant's Failure to Maintain.** If the Consultant fails to keep in effect at all times any insurance coverage required under this agreement, the SJVIA may, in addition to any other remedies it may have, suspend or terminate this agreement upon the occurrence of that failure, or purchase such insurance coverage, and charge the cost of that coverage to the Consultant. The SJVIA may offset such charges against any amounts owed by the SJVIA to the Consultant under this agreement.

Article 12
General Provisions

12.1 **Modification.** Except as provided in Article 4, this agreement may not be modified, and no waiver is effective, except by written agreement signed by both parties.

12.2 **Non-Assignment.** Neither party may assign its rights or delegate its obligations under this agreement without the prior written consent of the other party.

12.3 **Governing Law.** The laws of the State of California govern all matters arising from or related to this agreement.

12.4 **Jurisdiction and Venue.** This agreement is signed and performed in Fresno County, California. The Consultant consents to California jurisdiction for actions arising from or related to this agreement, and, subject to the Government Claims Act, all such actions must be brought and maintained in the Fresno County Superior Court.

12.5 **Construction.** The final form of this agreement is the result of the parties' combined efforts. If anything in this agreement is found by a court of competent jurisdiction to be ambiguous, that ambiguity shall not be resolved by construing the terms of this agreement against either party.

12.6 **Headings.** The headings and section titles in this agreement are for convenience only and are not part of this agreement.

12.7 **Severability.** If anything in this agreement is found by a court of competent jurisdiction to be unlawful or otherwise unenforceable, the balance of this agreement remains in effect, and the parties shall make best efforts to replace the unlawful or unenforceable part of

this agreement with lawful and enforceable terms intended to accomplish the parties' original intent.

12.8 **Nondiscrimination.** During the performance of this agreement, the Consultant shall not unlawfully discriminate against any employee or applicant for employment, or recipient of services, because of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, military status or veteran status pursuant to all applicable State of California and federal statutes and regulation.

12.9 **No Waiver.** Payment, change, waiver, or discharge by the SJVIA of any liability or obligation of the Consultant under this agreement on any one or more occasions is not a waiver of performance of any continuing or other obligation of the Consultant and does not prohibit enforcement by the SJVIA of any obligation on any other occasion.

12.10 **Entire Agreement.** This agreement, including its exhibits, is the entire agreement between the Consultant and the SJVIA with respect to the subject matter of this agreement, and it supersedes all previous negotiations, proposals, commitments, writings, advertisements, publications, and understandings of any nature unless those things are expressly included in this agreement. If there is any inconsistency between the terms of this agreement without its exhibits and the terms of the exhibits, then the inconsistency will be resolved by giving precedence first to the terms of this agreement without its exhibits, and then to the terms of the exhibits.

12.11 **No Third-Party Beneficiaries.** This agreement does not and is not intended to create any rights or obligations for any person or entity except for the parties.

12.12 **Authorized Signatures.** The Consultant represents and warrants to the SJVIA that:

(A) The Consultant is duly authorized and empowered to sign and perform its obligations under this agreement.

(B) The individual signing this agreement on behalf of the Consultant is duly authorized to do so and his or her signature on this agreement will legally bind the Consultant to the terms of this agreement.

12.13 **Counterparts.** This agreement may be signed in counterparts, each of which is an original, and all of which together constitute this agreement.

[*SIGNATURE PAGE FOLLOWS*]

The parties are signing this agreement on the date stated in the introductory clause.

CONSULTANT

_____
(Authorized signature)

_____
(Print name and title)

SAN JOAQUIN VALLEY INSURANCE AUTHORITY

_____
[Name of President]
President, Board of Directors

Reviewed and recommended for approval.

_____
SJVIA Manager