

1 **AMENDMENT NO. 1 TO SERVICE AGREEMENT**

2 This Amendment No. 1 to Service Agreement (“Amendment No. 1”) is dated
3 _____ and is between RDA Consulting, SPC, a California corporation
4 (“Contractor”), and the County of Fresno, a political subdivision of the State of California
5 (“County”).

6 **Recitals**

7 A. On December 12, 2023, the County and the Contractor entered into AB 109 Program
8 Evaluations, which is County agreement number A-23-669 (“Agreement”), for evaluation
9 services for programs funded by the Community Corrections Partnership (CCP).

10 B. To fulfill the scope of work outlined in the Agreement, the Contractor will require access
11 to data from programs funded by the CCP. This data is essential for collecting and analyzing
12 information to determine program effectiveness, as outlined in the Agreement. Therefore, a
13 separate Health Insurance Portability and Accountability (HIPAA) Business Associate
14 Agreement is necessary to establish clear guidelines and permissions for the Contractor to
15 request and receive relevant data from the Probation Department, community partners, and
16 other entities involved in CCP funded programs.

17 C. The Agreement references a Data Security Exhibit, but this exhibit was mislabeled in the
18 Agreement, and inadvertently omitted from the final document. To ensure data protection and
19 address security protocols, a properly labeled Data Security Exhibit E is being added to the
20 Agreement.

21 D. Contractor would like to include language in Exhibit B to allow Contractor to utilize staff,
22 whose rates are listed in Table B. Hourly Fee Schedule, to perform services listed in Table A.
23 Report Fees as necessary, not to exceed the annual budgeted amount.

24 E. The County and the Contractor now desire to amend the Agreement to make these
25 corrections and changes.

26 The parties therefore agree as follows:

27 1. Section 1.4 of the Agreement located on page 2, lines 3 and 4 is deleted in its entirety
28 and replaced with the following:

1 **“Confidential Information.** Contractor shall comply with all provisions of Exhibit
2 E, Data Security, attached and incorporated by this reference.”

3 2. A new Section 1.5 is added to the Agreement, as follows:

4 **“1.5 Health Insurance Portability and Accountability Act (HIPAA) Business**
5 **Associate Agreement.** Contractor agrees to and shall comply with all provisions
6 of Exhibit F, HIPAA Business Associate Agreement, attached and incorporated
7 by this reference.”

8 3. Exhibit B, Compensation of the Agreement located on page B-1, is deleted in its entirety
9 and replaced with the following:

10 “The Contractor shall be compensated for performance of its services under this
11 Agreement as provided in this Exhibit B. The Contractor is not entitled to any
12 compensation except as expressly provided in this Exhibit B. Table A. Report
13 Fees includes estimates of the hours and staff proposed for this Agreement. Staff
14 roles may be adjusted during the project to include billing for Table A tasks using
15 rates for other Contractor hourly staff, whose rates are included in Table B.
16 Hourly Fee Schedule. However, Contractor shall not exceed the total budgeted
17 amount in this Agreement. Contractor shall invoice monthly for all project
18 activities completed up to the agreed upon not-to-exceed budget total.”

19 4. When both parties have signed this Amendment No.1, the Agreement, and this
20 Amendment No. 1 together constitute the Agreement.

21 5. The Contractor represents and warrants to the County that:

22 a. The Contractor is duly authorized and empowered to sign and perform its obligations
23 under this Amendment No.1.

24 b. The individual signing this Amendment No.1 on behalf of the Contractor is duly
25 authorized to do so and his or her signature on this Amendment No.1 legally binds
26 the Contractor to the terms of this Amendment.

27 6. The parties agree that this Amendment No.1 may be executed by electronic signature as
28 provided in this section.

- 1 a. An “electronic signature” means any symbol or process intended by an individual
2 signing this Amendment to represent their signature, including but not limited to (1) a
3 digital signature; (2) a faxed version of an original handwritten signature; or (3) an
4 electronically scanned and transmitted (for example by PDF document) version of an
5 original handwritten signature.
- 6 b. Each electronic signature affixed or attached to this Amendment No. 1 (1) is deemed
7 equivalent to a valid original handwritten signature of the person signing this
8 Amendment for all purposes, including but not limited to evidentiary proof in any
9 administrative or judicial proceeding, and (2) has the same force and effect as the
10 valid original handwritten signature of that person.
- 11 c. The provisions of this section satisfy the requirements of Civil Code section 1633.5,
12 subdivision (b), in the Uniform Electronic Transaction Act (Civil Code, Division 3, Part
13 2, Title 2.5, beginning with section 1633.1).
- 14 d. Each party using a digital signature represents that it has undertaken and satisfied
15 the requirements of Government Code section 16.5, subdivision (a), paragraphs (1)
16 through (5), and agrees that each other party may rely upon that representation.
- 17 e. This Amendment No.1 is not conditioned upon the parties conducting the
18 transactions under it by electronic means and either party may sign this Amendment
19 with an original handwritten signature.

20 7. This Amendment No.1 may be signed in counterparts, each of which is an original, and
21 all of which together constitute this Amendment.

22 8. The Agreement as amended by this Amendment No. 1 is ratified and continued. All
23 provisions of the Agreement and not amended by this Amendment No. 1 remain in full force and
24 effect.

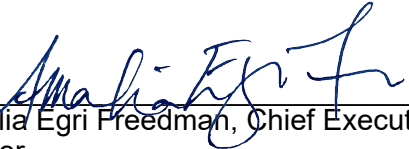
25 [SIGNATURE PAGE FOLLOWS]
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

The parties are signing this Amendment No. 1 on the date stated in the introductory clause.

RDA Consulting, SPC

COUNTY OF FRESNO



Amalia Egri Freedman, Chief Executive Officer

Nathan Magsig, Chairman of the Board of Supervisors of the County of Fresno

330 Franklin Street, Suite 40
Oakland, CA 94607

Attest:
Bernice E. Seidel
Clerk of the Board of Supervisors
County of Fresno, State of California

By: _____
Deputy

For accounting use only:

Org No.: 34300390
Account No.: 7295
Fund No.: 0001
Subclass No.: 10000

Exhibit E Data Security

1. Definitions

Capitalized terms used in this Exhibit E have the meanings set forth in this section 1.

- (A) **“Authorized Employees”** means the Contractor’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 Contractor’s subcontractors, representatives, agents, outsourcers, and consultants, and providers of professional services to the Contractor, 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 Exhibit E.
- (C) **“Director”** means the County’s Director of Internal Services/Chief Information Officer or his or her designee.
- (D) **“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.
- (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 Contractor by or upon the authorization of the County, 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 County relating to the Contractor’s (or any Authorized Person’s) privacy practices, or alleging a Security Breach. Such complaint shall have sufficient detail to enable the Contractor to promptly investigate and take remedial action under this Exhibit E.
- (H) **“Security Safeguards”** means physical, technical, administrative or organizational security procedures and practices put in place by the Contractor (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 3(C) of this Exhibit E.

Exhibit E
Data Security

- (I) **“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.
- (J) **“Use”** or any derivative of that word means to receive, acquire, collect, apply, manipulate, employ, process, transmit, disseminate, access, store, disclose, or dispose of Personal Information.

2. Standard of Care

- (A) The Contractor acknowledges that, in the course of its engagement by the County under this Agreement, the Contractor, or any Authorized Persons, may Use Personal Information only as permitted in this Agreement.
- (B) The Contractor acknowledges that Personal Information is deemed to be confidential information of, or owned by, the County (or persons from whom the County receives or has received Personal Information) and is not confidential information of, or owned or by, the Contractor, or any Authorized Persons. The Contractor further acknowledges that all right, title, and interest in or to the Personal Information remains in the County (or persons from whom the County receives or has received Personal Information) regardless of the Contractor’s, or any Authorized Person’s, Use of that Personal Information.
- (C) The Contractor agrees and covenants in favor of the Country that the Contractor shall:
 - (i) keep and maintain all Personal Information in strict confidence, using such degree of care under this section 2 as is reasonable and appropriate to avoid a Security Breach;
 - (ii) Use Personal Information exclusively for the purposes for which the Personal Information is made accessible to the Contractor pursuant to the terms of this Exhibit E;
 - (iii) not Use, Disclose, sell, rent, license, or otherwise make available Personal Information for the Contractor’s own purposes or for the benefit of anyone other than the County, without the County’s express prior written consent, which the County may give or withhold in its sole and absolute discretion; and
 - (iv) not, directly or indirectly, Disclose Personal Information to any person (an “Unauthorized Third Party”) other than Authorized Persons pursuant to this Agreement, without the Director’s express prior written consent.
- (D) Notwithstanding the foregoing paragraph, in any case in which the Contractor 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, Contractor shall (i) immediately notify the County of the specific demand for, and legal authority for the disclosure, including providing County with a copy of any notice, discovery demand, subpoena, or order, as applicable, received by the Contractor, or any Authorized Person, from any government regulatory authorities, or in relation to any legal proceeding, and (ii) promptly notify the County

Exhibit E Data Security

before such Personal Information is offered by the Contractor for such disclosure so that the County may have sufficient time to obtain a court order or take any other action the County may deem necessary to protect the Personal Information from such disclosure, and the Contractor shall cooperate with the County to minimize the scope of such disclosure of such Personal Information.

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

3. Information Security

- (A) The Contractor covenants, represents and warrants to the County that the Contractor'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 Contractor Uses credit, debit or other payment cardholder information, the Contractor 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 Contractor's sole cost and expense.
- (B) The Contractor covenants, represents and warrants to the County that, as of the effective date of this Agreement, the Contractor 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 Contractor's obligations under section 3(A) of this Exhibit E, the Contractor's (or Authorized Person's) Security Safeguards shall be no less rigorous than accepted industry practices and, at a minimum, include the following:
 - (i) limiting Use of Personal Information strictly to the Contractor's and Authorized Persons' technical and administrative personnel who are necessary for the Contractor's, or Authorized Persons', Use of the Personal Information pursuant to this Agreement;
 - (ii) ensuring that all of the Contractor's connectivity to County computing systems will only be through the County's security gateways and firewalls, and only through security procedures approved upon the express prior written consent of the Director;
 - (iii) 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)

Exhibit E Data Security

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 County'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 Director;

- (iv) 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 Director);
 - (v) strictly segregating Personal Information from all other information of the Contractor, including any Authorized Person, or anyone with whom the Contractor or any Authorized Person deals so that Personal Information is not commingled with any other types of information;
 - (vi) having a patch management process including installation of all operating system and software vendor security patches;
 - (vii) 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
 - (viii) providing appropriate privacy and information security training to Authorized Employees.
- (D) During the term of each Authorized Employee's employment by the Contractor, the Contractor shall cause such Authorized Employees to abide strictly by the Contractor's obligations under this Exhibit E. The Contractor shall maintain a disciplinary process to address any unauthorized Use of Personal Information by any Authorized Employees.
- (E) The Contractor shall, in a secure manner, backup daily, or more frequently if it is the Contractor's practice to do so more frequently, Personal Information received from the County, and the County shall have immediate, real time access, at all times, to such backups via a secure, remote access connection provided by the Contractor, through the Internet.
- (F) The Contractor shall provide the County 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 County's primary security contact with the Contractor and shall be

Exhibit E Data Security

available to assist the County twenty-four (24) hours per day, seven (7) days per week as a contact in resolving the Contractor's and any Authorized Persons' obligations associated with a Security Breach or a Privacy Practices Complaint.

- (G) The Contractor 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 within, or otherwise impair any County computing system, with or without the intent to cause harm.

4. Security Breach Procedures

- (A) Immediately upon the Contractor's awareness or reasonable belief of a Security Breach, the Contractor shall (i) notify the Director 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) 600-6200 / servicedesk@fresnocountyca.gov (which telephone number and email address the County may update by providing notice to the Contractor), 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 Contractor's notification to the County of a Security Breach, as provided pursuant to section 4(A) of this Exhibit E, the Parties shall coordinate with each other to investigate the Security Breach. The Contractor agrees to fully cooperate with the County, including, without limitation:
- (i) assisting the County in conducting any investigation;
 - (ii) providing the County with physical access to the facilities and operations affected;
 - (iii) facilitating interviews with Authorized Persons and any of the Contractor's other employees knowledgeable of the matter; and
 - (iv) 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 County.

To that end, the Contractor 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 County, and the Contractor shall provide a written report of the investigation and reporting required to the Director within 30 days after the Contractor's discovery of the Security Breach.

- (C) County shall promptly notify the Contractor of the Director's knowledge, or reasonable belief, of any Privacy Practices Complaint, and upon the Contractor's receipt of that notification, the Contractor shall promptly address such Privacy Practices Complaint, including taking any corrective action under this Exhibit E, all at the Contractor's sole expense, in accordance with applicable privacy rights, laws, regulations and standards.

Exhibit E Data Security

In the event the Contractor discovers a Security Breach, the Contractor shall treat the Privacy Practices Complaint as a Security Breach. Within 24 hours of the Contractor's receipt of notification of such Privacy Practices Complaint, the Contractor shall notify the County 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 for that determination.

- (D) The Contractor 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 Contractor's sole expense, in accordance with applicable privacy rights, laws, regulations and standards. The Contractor shall reimburse the County for all reasonable costs incurred by the County in responding to, and mitigating damages caused by, any Security Breach, including all costs of the County incurred relation to any litigation or other action described section 4(E) of this Exhibit E.
- (E) The Contractor agrees to cooperate, at its sole expense, with the County in any litigation or other action to protect the County's rights relating to Personal Information, including the rights of persons from whom the County receives Personal Information.

5. Oversight of Security Compliance

- (A) The Contractor shall have and maintain a written information security policy that specifies Security Safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities.
- (B) Upon the County's written request, to confirm the Contractor's compliance with this Exhibit E, as well as any applicable laws, regulations and industry standards, the Contractor grants the County or, upon the County's election, a third party on the County's behalf, permission to perform an assessment, audit, examination or review of all controls in the Contractor's physical and technical environment in relation to all Personal Information that is Used by the Contractor pursuant to this Agreement. The Contractor shall fully cooperate with such assessment, audit or examination, as applicable, by providing the County or the third party on the County's behalf, access to all Authorized Employees and other knowledgeable personnel, physical premises, documentation, infrastructure and application software that is Used by the Contractor for Personal Information pursuant to this Agreement. In addition, the Contractor shall provide the County with the results of any audit by or on behalf of the Contractor that assesses the effectiveness of the Contractor's information security program as relevant to the security and confidentiality of Personal Information Used by the Contractor or Authorized Persons during the course of this Agreement under this Exhibit E.
- (C) The Contractor shall ensure that all Authorized Persons who Use Personal Information agree to the same restrictions and conditions in this Exhibit E. that apply to the Contractor with respect to such Personal Information by incorporating the relevant provisions of these provisions into a valid and binding written agreement between the Contractor and such Authorized Persons, or amending any written agreements to provide same.

Exhibit E Data Security

6. Return or Destruction of Personal Information. Upon the termination of this Agreement, the Contractor shall, and shall instruct all Authorized Persons to, promptly return to the County 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 County at the time of such return, or upon the express prior written consent of the Director, securely destroy all such Personal Information, and certify in writing to the County that such Personal Information have been returned to the County or disposed of securely, as applicable. If the Contractor is authorized to dispose of any such Personal Information, as provided in this Exhibit E, such certification shall state the date, time, and manner (including standard) of disposal and by whom, specifying the title of the individual. The Contractor shall comply with all reasonable directions provided by the Director with respect to the return or disposal of Personal Information and copies of Personal Information. If return or disposal of such Personal Information or copies of Personal Information is not feasible, the Contractor shall notify the County according, specifying the reason, and continue to extend the protections of this Exhibit E to all such Personal Information and copies of Personal Information. The Contractor shall not retain any copy of any Personal Information after returning or disposing of Personal Information as required by this section 6. The Contractor's obligations under this section 6 survive the termination of this Agreement and apply to all Personal Information that the Contractor retains if return or disposal is not feasible and to all Personal Information that the Contractor may later discover.

7. Equitable Relief. The Contractor acknowledges that any breach of its covenants or obligations set forth in this Exhibit E may cause the County irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the County 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 County 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 County at law or in equity or under this Agreement.

8. Indemnity. The Contractor shall defend, indemnify and hold harmless the County, its officers, employees, and agents, (each, a "**County 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 Exhibit E and the cost of pursuing any insurance providers, arising out of or resulting from any third party claim or action against any County Indemnitee in relation to the Contractor's, its officers, employees, or agents, or any Authorized Employee's or Authorized Person's, performance or failure to perform under this Exhibit E or arising out of or resulting from the Contractor's failure to comply with any of its obligations under this section 8. The provisions of this section 8 do not apply to the acts or omissions of the County. The provisions of this section 8 are cumulative to any other obligation of the Contractor to, defend, indemnify, or hold harmless any County Indemnitee under this Agreement. The provisions of this section 8 shall survive the termination of this Agreement.

Exhibit E
Data Security

9. Survival. The respective rights and obligations of the Contractor and the County as stated in this Exhibit E shall survive the termination of this Agreement.

10. No Third Party Beneficiary. Nothing express or implied in the provisions of in this Exhibit E is intended to confer, nor shall anything in this Exhibit E confer, upon any person other than the County or the Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

11. No County Warranty. The County does not make any warranty or representation whether any Personal Information in the Contractor's (or any Authorized Person's) possession or control, or Use by the Contractor (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.

Health Insurance Portability and Accountability Act (HIPAA)
Business Associate Agreement

The County of Fresno (“County”) has contracted with RDA Consulting, SPC (“Contractor”) for Justice Assistance Grant Program Evaluation Services pursuant to Procurement Agreement P-24-064, dated February 8, 2024 (“Procurement Agreement”). The County and the Contractor agree that this Business Associate Agreement (“BAA” or the “Agreement”) is incorporated into the Procurement Agreement and is subject to all of its terms and requirements, in addition to the terms and requirements contained in this BAA.

1. The County is a “Covered Entity,” and the Contractor is a “Business Associate,” as these terms are defined by 45 CFR 160.103. In connection with providing services under the Agreement, the parties anticipate that the Contractor will create and/or receive Protected Health Information (“PHI”) from or on behalf of the County. The parties enter into this BAA to comply with the Business Associate requirements of HIPAA, to govern the use and disclosures of PHI under this Agreement. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and 164.

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 California Welfare and Institutions Code sections 5328, 10850, and 14100.2 et seq.; 42 CFR 2; 42 CFR 431; California Civil Code section 56 et seq.; the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”), including, but not limited to, 45 CFR Parts 160, 45 CFR 162, and 45 CFR 164; the Health Information Technology for Economic and Clinical Health Act (“HITECH”) regarding the confidentiality and security of patient information, including, but not limited to 42 USC 17901 et seq.; and the Genetic Information Nondiscrimination Act (“GINA”) of 2008 regarding the confidentiality of genetic information.

Except as otherwise provided in this Agreement, the Contractor, as a business associate of the County, may use or disclose Protected Health Information (“PHI”) to perform functions,

activities or services for or on behalf of the County, as specified in this Agreement, provided that such use or disclosure shall not violate HIPAA Rules. The uses and disclosures of PHI may not be more expansive than those applicable to the County, as the “Covered Entity” under the HIPAA Rules, except as authorized for management, administrative or legal responsibilities of the Contractor.

2. The Contractor, including its subcontractors and employees, shall protect from unauthorized access, use, or disclosure of names and other identifying information, including genetic information, concerning persons receiving services pursuant to this Agreement, except where permitted in order to carry out data aggregation purposes for health care operations [45 CFR §§ 164.504(e)(2)(i), 164.504(e)(2)(ii)(A), and 164.504(e)(4)(i)]. This pertains to any and all persons receiving services pursuant to a County-funded program. This requirement applies to electronic PHI. The Contractor shall not use such identifying information or genetic information for any purpose other than carrying out the Contractor’s obligations under this Agreement.

3. The Contractor, including its 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 of the United States Department of Health and Human Services (“Secretary”), or authorized by the client/patient in writing. In using or disclosing PHI that is permitted by this Agreement or authorized by law, the Contractor shall make reasonable efforts to limit PHI to the minimum necessary to accomplish intended purpose of use, disclosure or request.

4. For purposes of the above sections, identifying information shall include, but not be limited to, name, identifying number, symbol, or other identifying particular assigned to the individual, such as fingerprint or voiceprint, or photograph.

5. For purposes of the above sections, genetic information shall include genetic tests of family members of an individual or individual(s), manifestation of disease or disorder of family members of an individual, or any request for or receipt of genetic services by individual or

family members. Family member means a dependent or any person who is first, second, third, or fourth degree relative.

6. The Contractor shall provide access, at the request of the County, and in the time and manner designated by the County, to PHI in a designated record set (as defined in 45 CFR § 164.501), to an individual or to COUNTY in order to meet the requirements of 45 CFR § 164.524 regarding access by individuals to their PHI. With respect to individual requests, access shall be provided within thirty (30) days from request. Access may be extended if the Contractor cannot provide access and provides the individual with the reasons for the delay and the date when access may be granted. PHI shall be provided in the form and format requested by the individual or the County.

The Contractor shall make any amendment(s) to PHI in a designated record set at the request of the County or individual, and in the time and manner designated by the County in accordance with 45 CFR § 164.526.

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

7. The Contractor shall report to the County, 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 the Contractor becomes aware, immediately and without reasonable delay and in no case later than two (2) business days of discovery. Immediate notification shall be made to the County's Information Security Officer and Privacy Officer and the County's Department of Public Health ("DPH") HIPAA Representative, within two (2) business days of discovery. 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 Contractor shall take prompt corrective action to cure any deficiencies and any action pertaining to such unauthorized disclosure required by applicable federal and State laws and regulations.

The Contractor shall investigate such breach and is responsible for all notifications required by law and regulation or deemed necessary by the County and shall provide a written report of the investigation and reporting required to the County's Information Security Officer and Privacy Officer and the County's DPH HIPAA Representative.

This written investigation and description of any reporting necessary shall be postmarked within the thirty (30) working days of the discovery of the breach to the addresses below:

County of Fresno
Department of Public Health
HIPAA Representative
(559) 600-6439
P.O. Box 11867
Fresno, California 93775

County of Fresno
Department of Public Health
Privacy Officer
(559) 600-6405
P.O. Box 11867
Fresno, California 93775

County of Fresno
Department of Internal
Services
Information Security Officer
(559) 600-5800
2048 North Fine Street
Fresno, California 93727

8. The Contractor shall make its internal practices, books, and records relating to the use and disclosure of PHI received from the county, or created or received by the Contractor on behalf of the County, in compliance with Parts the HIPAA Rules. The Contractor shall make its internal practices, books, and records relating to the use and disclosure of PHI received from the County, or created or received by the Contractor on behalf of the County, available to the Secretary upon demand.

The Contractor shall cooperate with the compliance and investigation reviews conducted by the Secretary. PHI access to the Secretary must be provided during the Contractor's normal business hours; however, upon exigent circumstances access at any time must be granted. Upon the Secretary's compliance or investigation review, if PHI is unavailable to the Contractor and in possession of a subcontractor of the Contractor, the Contractor must certify to the Secretary its efforts to obtain the information from the subcontractor.

9. **Safeguards**

The Contractor 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 protect the confidentiality, integrity, and availability of PHI, including electronic

PHI, that it creates, receives, maintains or transmits on behalf of the County and to prevent unauthorized access, viewing, use, disclosure, or breach of PHI other than as provided for by this Agreement. The Contractor shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI. The Contractor 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 Contractor's operations and the nature and scope of its activities. Upon the County's request, the Contractor shall provide the County with information concerning such safeguards.

The Contractor 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. Said 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 (8) characters or more in length;
- (2) Changed every ninety (90) days;
- (3) Changed immediately if revealed or compromised; and
- (4) Composed of characters from at least three (3) of the following four (4) groups from the standard keyboard:
 - a) Upper case letters (A-Z);
 - b) Lowercase letters (a-z);

- c) Arabic numerals (0 through 9); and
- d) Non-alphanumeric characters (punctuation symbols).

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

1. Network-based firewall and/or personal firewall;
2. Continuously updated anti-virus software; and
3. Patch management process including installation of all operating system/software vendor security patches.

The Contractor shall utilize 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).

The Contractor 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 Contractor must apply appropriate sanctions against its employees who fail to comply with these safeguards. The Contractor must adopt procedures for terminating access to PHI when employment of employee ends.

10. Mitigation of Harmful Effects

The Contractor shall mitigate, to the extent practicable, any harmful effect that is suspected or known to the Contractor of an unauthorized access, viewing, use, disclosure, or breach of PHI by the Contractor or its subcontractors in violation of the requirements of these provisions. The Contractor must document suspected or known harmful effects and the outcome.

11. The Contractor's Subcontractors

The Contractor shall ensure that any of its contractors, including subcontractors, if applicable, to whom the Contractor provides PHI received from or created or received by the

Contractor on behalf of the County, agree to the same restrictions, safeguards, and conditions that apply to the Contractor 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.

Nothing in this section 11 or this exhibit authorizes the Contractor to perform services under this Agreement using subcontractors.

12. Employee Training and Discipline

The Contractor shall train and use reasonable measures to ensure compliance with the requirements of these provisions by employees who assist in the performance of functions or activities on behalf of the County under this Agreement and use or disclose PHI, and discipline such employees who intentionally violate any provisions of these provisions, which may include termination of employment.

13. Termination for Cause

Upon the County's knowledge of a material breach of these provisions by the Contractor, the County will either:

A. Provide an opportunity for the Contractor to cure the breach or end the violation, and the County may terminate this Agreement if the Contractor does not cure the breach or end the violation within the time specified by the County; or

B. Immediately terminate this Agreement if the Contractor has breached a material term of this exhibit and cure is not possible, as determined by the County.

C. If neither cure nor termination is feasible, the County's Privacy Officer will report the violation to the Secretary of the U.S. Department of Health and Human Services.

14. Judicial or Administrative Proceedings

The County may terminate this Agreement if: (1) the Contractor 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 in an administrative or civil proceeding in which the Contractor is a party that the Contractor has violated a privacy or security standard or requirement of the HITECH Act, HIPAA or other security or privacy laws.

15. Effect of Termination

Upon termination or expiration of this Agreement for any reason, the Contractor shall return or destroy all PHI received from the County (or created or received by the Contractor on behalf of the County) that the Contractor still maintains in any form, and shall retain no copies of such PHI. If return or destruction of PHI is not feasible, the Contractor 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 Contractor. If the Contractor destroys the PHI data, a certification of date and time of destruction shall be provided to the County by the Contractor.

16. Compliance with Other Laws

To the extent that other state and/or federal laws provide additional, stricter and/or more protective privacy and/or security protections to PHI or other confidential information covered under this BAA, the Contractor agrees to comply with the more protective of the privacy and security standards set forth in the applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA Rules or are otherwise more favorable to the individual.

17. Disclaimer

The County makes no warranty or representation that compliance by the Contractor with these provisions, the HITECH Act, or the HIPAA Rules, will be adequate or satisfactory for the Contractor's own purposes or that any information in the Contractor's possession or control, or transmitted or received by the Contractor, is or will be secure from unauthorized access, viewing, use, disclosure, or breach. The Contractor is solely responsible for all decisions made by the Contractor regarding the safeguarding of PHI.

18. Amendment

The parties acknowledge that Federal and State laws relating to electronic data security and privacy are rapidly evolving and that amendment of this exhibit 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 the HIPAA Rules, the HITECH Act and other applicable laws relating to the security or privacy of PHI. The County may terminate this Agreement upon thirty (30) days written notice in the event that the Contractor does not enter into an amendment providing assurances regarding the safeguarding of PHI that the County in its sole discretion, deems sufficient to satisfy the standards and requirements of the HIPAA Rules, and the HITECH Act.

19. No Third-Party Beneficiaries

Nothing expressed or implied in the provisions of this exhibit is intended to confer, and nothing in this exhibit does confer, upon any person other than the County or the Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

20. Interpretation

The provisions of this exhibit shall be interpreted as broadly as necessary to implement and comply with the HIPAA Rules, and applicable State 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 the HIPAA Rules.

21. Regulatory References

A reference in the terms and conditions of these provisions to a section in the HIPAA Rules means the section as in effect or as amended.

22. Survival

The respective rights and obligations of the Contractor as stated in this exhibit survive the termination or expiration of this Agreement.

23. No Waiver of Obligation

Change, waiver or discharge by the County of any liability or obligation of the Contractor under this exhibit on any one or more occasions is not a waiver of performance of any continuing or other obligation of the Contractor and does not prohibit enforcement by the County of any obligation on any other occasion.