

**SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA**



**ITEM: 3.15
(ID # 20623)**

MEETING DATE:
Tuesday, December 06, 2022

FROM : PUBLIC SOCIAL SERVICES:

SUBJECT: DEPARTMENT OF PUBLIC SOCIAL SERVICES: Approve and Execute Agreement DPSS-0004647 with Binti, Inc. for Placement Services Software through June 30, 2027; All Districts. [Total Cost \$2,102,000 and up to \$420,400 in additional compensation; Funding: Federal 24%; General Fund 24%; Realignment 52%]

RECOMMENDED MOTION: That the Board of Supervisors:

1. Approve Agreement DPSS-0004647 with Binti, Inc. for Placement Services Software, in the total aggregate amount of \$2,102,000, effective upon execution through June 30, 2027; and authorize the Chair of the Board to sign the Agreement on behalf of the County.
2. Authorize the Purchasing Agent, in accordance with Ordinance No. 459, based on the availability of funding and as approved as to form by County Counsel to: (a) sign amendments that make modifications to the Scope of Services that stay within the intent of the agreement, and (b) sign amendments to the compensation provisions that do not exceed the sum total of \$420,400.

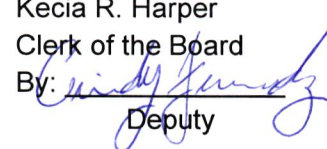
ACTION:Policy, H-11


Sayori Baldwin, DPSS Director 11/17/2022

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Spiegel, seconded by Supervisor Perez and duly carried by unanimous vote, IT WAS ORDERED that the above matter is approved as recommended.

Ayes: Jeffries, Spiegel, Washington, Hewitt, and Perez
Nays: None
Absent: None
Date: December 6, 2022
xc: DPSS

Kecia R. Harper
Clerk of the Board
By: 
Deputy

**SUBMITTAL TO THE BOARD OF SUPERVISORS COUNTY OF RIVERSIDE,
STATE OF CALIFORNIA**

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	\$ 250,000	\$ 463,000	\$ 2,102,000	\$ 0
NET COUNTY COST	\$ 60,000	\$ 111,120	\$ 504,480	\$ 0
SOURCE OF FUNDS: Federal 24%; General Fund 24%; Realignment 52%			Budget Adjustment: No	
			For Fiscal Year: 22/23 – 26/27	

C.E.O. RECOMMENDATION: Approve

BACKGROUND:

Summary

The Department of Public Social Services (DPSS) Children’s Services Division (CSD) is charged with finding suitable and stable placements for youth removed from their homes due to abuse and/or neglect or experiencing placement disruption. Suitable and stable placements are coordinated based on the needs and familiar resources available to each youth. Sourcing for placement is a complex process as each youth has different behavioral, physical, and social needs. The current climate for finding stable placements presents limited options/resources, which at times also presents several delays.

Under California’s Resource Family Approval (RFA) program, all relative and non-relative caregivers (resource families) complete the same set of activities to obtain approval to be foster or adoptive parents. The RFA program within Children’s Services Division (CSD) work with resource families to complete personal, health and home assessments, training, and criminal background clearances in order to ensure that homes are safe and appropriate for placement of dependent children. This approval process is very complex and requires the gathering of data at various milestones; therefore, the accurate and comprehensive tracking of data is key.

DPSS requests to enter into an agreement with Binti for a web-based software that provides a database for RFA approval tracking and placement sourcing. Binti Software will allow social work staff to enter data, complete/capture documentation, track individual family progress and match youth with available homes. The Binti Placement Software solution will increase effectiveness and efficiency of sourcing for placement through the following functions:

- Electronic completion, submittal, and editing of the Form 738 (Request for Placement Search)
- Monitoring of placement searches
- Supervisor and managerial oversight to monitor the workload and assign searches to staff
- Real-time updates to case carrying social workers by providing individual log-in abilities where the case worker can see the search efforts

**SUBMITTAL TO THE BOARD OF SUPERVISORS COUNTY OF RIVERSIDE,
STATE OF CALIFORNIA**

- Placement “matching” based on key characteristics of a youth and a family; gender, age, level of care required, community/school of origin, and other key factors/variables; thus, resulting in a short list of potential placement providers
- Ability to send an initial text/email to a short list of providers to determine capacity and eligibility for placement
- Note entry for real time tracking of the outcome of a placement conversation, acceptance, denial, reason for denial, etc.
- Reporting functions that provide data related to key performance indicators.

Binti partnered with San Francisco's Human Services Agency /Department of Family and Children's Services as a result of a Request for Proposal (RFP) through the San Francisco Mayor's Office of Civic Innovation 2016 Startup in Residence Program. Through this collaboration, Binti developed and delivered a specialized interactive, mobile, web-based tool that automates the RFA process by allowing resource families and child welfare staff to enter information, upload and approve documents and track the progress or resource families ultimately to approval status. Currently, forty-one (41) of the 58 counties in California contract with Binti for this software/service.

Binti's RFA software is the only commercial off-the-shelf product specifically designed to be compatible with the existing State of California Welfare Services (CWS) Case Management System (CMS) and has been customized to work with CMS. Binti offers families and CSD staff with website, tablet and mobile device access, and will interface with CMS.

Impact on Residents and Businesses

The Binti Software Solution will facilitate effective and efficient RFA processes and searches for long-term placement of DPSS youth and non-minor dependents, subsequently reducing the amount of time youth are in transition awaiting placement.

Additional Fiscal Information

The total payments to Binti, Inc. shall not exceed:

CONTRACT TERM	ANNUAL PAYMENT
Upon Execution through June 30, 2023	\$250,000
July 1, 2023 through June 30, 2024	\$463,000
July 1, 2024 through June 30, 2025	\$463,000
July 1, 2025 through June 30, 2026	\$463,000
July 1, 2026 through June 30, 2027	\$463,000
Total	\$2,102,000

All funds are within the current approved budget. There is no additional net county cost.

SUBMITTAL TO THE BOARD OF SUPERVISORS COUNTY OF RIVERSIDE,
STATE OF CALIFORNIA


Contract History and Price Reasonableness

General market, commercial off-the-shelf software products vary with specificity and compatibility, in this case the RFA process and CWC/CMS: nonetheless, as to the extent that these types of purchases may be compared, Binti's process/fees are comparable to those in the general market.

ATTACHMENTS:

Attachment A: Agreement DPSS-0004647 with Binti, Inc. for Placement Services Software

Attachment B: Approved Sole Source Justification (SSJ) Form


Suzanna Hickley, Assistant Director of Purchasing and Fleet Service 11/17/2022


Erianna Lontajo, Principal Management Analyst 11/29/2022


Jim Smith, Chief Information Officer 11/17/2022

MASTER SUBSCRIPTION AND SERVICES AGREEMENT

This Master Subscription and Services Agreement ("**Agreement**") is made as of December 6, 2022 ("**Effective Date**"), between Binti, Inc., a Delaware corporation, with an address at 1212 Broadway, Suite 200, Oakland, California 94612 ("**Binti**"), and the County of Riverside, a political subdivision of the State of California, on behalf of its Department of Public Social Services, with an address at 4060 County Circle Dr, Riverside, California 92503 ("**Licensee**"). Binti and Licensee will be referenced to individually herein as "**Party**" and collectively as the "**Parties**."

Binti has developed a Software-as-a-Service platform, as described at www.binti.com ("**Platform**"). The Approvals Platform allows users to apply online to become approved to foster children and allows social workers to manage their approval workflow online. The Placements Platform allows for the matching of child referrals to approved foster families ("**Authorized Purpose**"). This Agreement governs a relationship whereby Binti will (i) grant Licensee access to the Platform; and (ii) perform the professional services set forth in **Exhibit A** attached hereto ("**Professional Services**," together with the Platform, the "**Services**"). Accordingly, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. Proprietary Rights.

(a) **Platform.** Subject to the terms and conditions of this Agreement, Binti hereby grants to Licensee during the Term (defined below) a non-exclusive, non-transferable and non-sublicensable license to allow its employees and contractors who have been issued valid access credentials from Binti ("**Authorized Users**") to access and use the Platform solely to help facilitate foster care and adoptions for children. Binti will provide access to the Service to Authorized Users subject to Binti's Terms of Service, and in its capacity as a data controller, will process the Authorized Users' personal information in compliance with Binti's Privacy Policy. Binti will provide Licensee with the support services set forth in **Exhibit B** attached hereto.

(b) **Restrictions.** Licensee will not, and will not permit any third party to: (i) copy, modify, translate, or create derivative works of the Platform; (ii) reverse engineer, decompile, disassemble or otherwise attempt to reconstruct, identify or discover any source code, underlying ideas, underlying user interface techniques, or algorithms of the Platform (except to the extent such prohibition is contrary to applicable law); (iii) lend, lease, offer for sale, sell or otherwise use the Platform for the benefit of any third party except as permitted under Section 1(a); (iv) attempt to disrupt the integrity or performance of the Platform; (v) attempt to gain unauthorized access to the Platform or its related systems or networks; or (vi) use the Platform in a manner that violates this Agreement, any third party rights or any applicable laws, rules or regulations.

(c) **Binti Ownership.** Except for the rights granted to Licensee in Section 1(a) above and Licensee's rights to Data (defined below), as between the Parties, Binti retains all right, title and interest, including all intellectual property rights, in and to the Platform (including all Updates thereto) and all aggregated and de-identified information that Binti's systems or applications automatically collect regarding the Platform and/or its use and/or performance (including, without limitation, de-identified Data that does not, and cannot reasonably be used to, identify Licensee or any individual) ("**Diagnostic Data**") (which, notwithstanding anything to the contrary, Binti may fully exploit). All rights that Binti does not expressly grant to Licensee in this Section 1 are reserved and Binti does not grant any implied licenses under this Section 1.

(d) **Licensee Ownership.** As between the Parties, Licensee owns all data, information and other materials submitted to the Platform or Binti by Licensee or Authorized Users (which, for clarity, excludes Diagnostic Data) (collectively, "**Data**"). Licensee represents and warrants that: (i) it either owns the Data or is otherwise permitted to grant the license set forth in this Section; (ii) the posting and use of Data on or through the Platform does not violate the privacy rights, publicity rights, copyrights, contract rights, intellectual property rights, or any other rights of any person; and (iii) the posting of Data on the Platform does not result in a breach of contract between Licensee and any third party. Licensee hereby grants to Binti a non-exclusive and non-transferable (except under Section 10) license to use and host the Data, solely to provide the Services. Binti is not responsible for the content of any Data or the way Licensee or its Authorized Users choose to use the Platform to store or process any Data. Upon termination or expiration of this Agreement for any reason, Binti will permit Licensee to download all Data from the Platform in .csv format.

2. Use of the Services.

(a) **Binti's Obligations.** Binti will use commercially reasonable efforts to make the Service available at all times, except for planned downtime and any unavailability caused by Force Majeure Events (defined below). If the Platform monthly availability averages less than 99.5% for three or more months in a rolling twelve month period, Licensee may terminate this Agreement for material breach. Binti will provide Licensee with reasonable advanced written notice of any major upgrade or changes that will materially adversely affect the Platform availability. Binti will maintain commercially reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Data.

(b) Binti shall provide Licensee reasonable access to Platform security logs, latency statistics, and other related security data related to the Service and Data at no cost to Licensee.

(c) Licensee's Obligations. Licensee acknowledges and agrees that it is responsible for the use or misuse of the Service by Authorized Users, and a breach by any Authorized User of any term of this Agreement will be deemed a breach by Licensee of this Agreement. Licensee acknowledges and agrees that the Licensee and Licensee's Authorized Users use of the Platform is in compliance with all applicable laws, and Licensee acknowledges that Licensee assumes all risk arising from any such use that is not compliant with applicable laws.

3. Professional Services.

(a) General. Subject to Licensee's compliance with the terms and conditions of this Agreement, Binti will perform the Professional Services in accordance with any specifications set forth in Exhibit A. Each Party will communicate with the point of contact set forth in Exhibit A in connection with the Professional Services. Licensee will reasonably cooperate with Binti to facilitate provision of Professional Services. This cooperation will include, without limitation, (i) performing any tasks reasonably necessary for Binti to provide the Professional Services and to avoid unnecessary delays; (ii) fulfilling any Licensee obligations described in Exhibit A in a timely manner; and (iii) responding to Binti's reasonable requests related to Professional Services in a timely manner. Notwithstanding anything in Exhibit A to the contrary, Binti will not be liable for any delays in performing the Professional Services that arise, in whole or in part, from Licensee's acts or omissions, including, without limitation, its failure to comply with this Section 3(a).

(b) Intellectual Property Rights. Binti solely owns all right, title and interest in and to any software, notes, records, drawings, designs or other copyrightable materials, inventions (whether or not patentable), improvements, developments, discoveries and trade secrets conceived, discovered, authored, invented, developed or reduced to practice by Binti, solely or in collaboration with others, arising out of, or in connection with, Binti performing the Professional Services, including any copyrights, patents, trade secrets, mask work rights or other intellectual property rights relating to the foregoing ("Inventions"). Binti hereby grants to Licensee a non-exclusive, non-transferable, non-sublicensable, royalty-free and worldwide right during the Term to use the portion of the Inventions that is incorporated into any deliverables that Binti provides to Licensee under Exhibit A solely to use any such deliverables. Binti reserves all rights not expressly granted in the prior sentence and does not grant any implied licensed under this Section 3.

4. Fees.

(a) Fees. During the Initial Implementation (as defined in Exhibit A, Attachment II) phase, upon the "Acceptance" (as defined in Exhibit A, 2(a)) of each Milestone (as set forth in Exhibit A, Attachment II, Section B), Licensee will pay Binti the corresponding payment amount as set forth therein. At "Full Implementation" (as defined in Attachment II) of all milestones as set forth in Section 2(a) of Exhibit A hereto, Licensee will pay Binti a pro-rated annual fee for the remainder of the then current fiscal year in advance calculated as follows: divide the number of days remaining in the then current fiscal year (which begins on July 1st and ends on June 30th) by 365 days, then multiply that percentage by \$463,000. After full implementation, the annual full fee may be increased up to 5% annually, subject to Binti and DPSS approval, by way of written amendment. By request of DPSS in connection with enhancements and/or improvements made to the Platform or Professional Services, Binti may increase the Fees by an amount deemed necessary by Binti, subject to DPSS' approval upon sixty (60) days prior written notice. Any changes to fees must be made by way of written amendment. Subject to the preceding sentence, thereafter, in advance of each subsequent fiscal year through June 30, 2027, Binti will be paid \$463,000 for access to the RFA Approvals Module, Placement/Matching Module and Public Recruiting Website, unless terminated earlier (collectively, "Fees"). Licensee shall pay Binti for services performed, products provided, or expenses incurred in accordance with Attachment II, Fiscal Provisions, section B. Licensee is not responsible for any fees or costs incurred above or beyond the contracted amount and shall have no obligation to purchase any specified amount of services or product. Unless otherwise specifically stated in Attachment II, Licensee shall not be responsible for payment of any of Binti's expenses related to this Agreement. All Fees will be due and payable within sixty (60) days from the date of the applicable invoice issued by Binti. Invoices shall be submitted via email to: ClientServicesContracts@rivco.org.

(1) The obligation of Licensee for payment under this Agreement beyond the current fiscal year is contingent upon and limited by the availability of County funding from which payment can be made. Subject to the last sentence of the paragraph, there shall be no legal liability for payment on the part of Licensee beyond June 30 of each year unless funds are made available for such payment by the County Board of Supervisors. In the event such funds are not forthcoming for any reason, Licensee shall immediately notify Binti in writing and this Agreement shall be deemed terminated effective as of the notification date. Licensee shall make all payments to Binti that were properly earned prior to the notice of the unavailability of funding.

(b) Taxes. The Fees do not include any taxes, levies, duties or similar governmental assessments of any nature, including, for example, value-added, sales, use or withholding taxes, assessable by any applicable taxing authorities

(collectively, "**Taxes**"). Licensee is responsible for paying all Taxes associated with its receipt of the Services (except for any Taxes based on Binti's net income).

5. Confidential Information.

(a) Definition of Confidential Information. As used herein, "**Confidential Information**" means all confidential information disclosed by a Party ("**Disclosing Party**") to the other Party ("**Receiving Party**"), that is marked in writing as "confidential" or by a similar designation. For clarity, Confidential Information of Binti also includes the Binti technology underlying the Platform and any related non-public specifications, documentation or technical information that Binti makes available to Licensee. Confidential Information will not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (ii) was known to the Receiving Party without restriction prior to its disclosure by the Disclosing Party and without breach of any obligation owed to the Disclosing Party; (iii) is received from a third party without restriction and without breach of any obligation owed to the Disclosing Party; or (iv) was independently developed by the Receiving Party without use of or reference to any Confidential Information of the Disclosing Party.

(b) Protection of Confidential Information. The Receiving Party will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care). The Receiving Party may only use Confidential Information of the Disclosing Party to perform its obligations or exercise its rights under this Agreement. Except as expressly authorized by the Disclosing Party in writing, the Receiving Party will limit access to Confidential Information of the Disclosing Party to those of its and its affiliates' employees, contractors or agents who need such access to perform obligations under this Agreement and who agree to abide by the terms set forth in this Section 5.

(c) Required Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party if it is required by law to do so. The Receiving Party will give the Disclosing Party prior notice of disclosure (to the extent legally permitted).

(d) Breach Notification: Upon discovery or reasonable belief of any Data breach, Binti shall notify Licensee via email to DPSS Privacy Officer at privacyincident@rivco.org forty-eight (48) hours after discovery. Binti shall, include in the notification as it becomes available: (i) the nature of the breach, (ii) the Data accesses, used, disclosed, or otherwise compromised; (iii) the person(s) who accessed, used, disclosed, and/or received the Data; (iv) actions Binti has or will take to quarantine and mitigate further damages; and (v) corrective action Binti has or will take to prevent future breaches.

(e) Health Insurance Portability Accountability Act: Binti is subject to and shall operate in compliance with all relevant requirements contained in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, enacted August 21, 1996, and the related laws and regulations promulgated subsequent thereto. The parties agree to the terms and conditions the HIPAA Business Associated attached as Attachment III.

(f) Personally Identifiable Information:

1. Personally Identifiable Information (PII) refers to personally identifiable information that can be used alone or in conjunction with any other reasonably available information, to identify a specific individual. PII includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. The PII may be electronic, paper, verbal, or recorded. PII may collected performing administrative functions on behalf of programs, such as determining eligibility for, or enrollment in, and collecting PII for such purposes, to the extent such activities are authorized by law.

2. Binti may use or disclose PII only to perform functions, activities or services directly related to the administration of programs in accordance with Welfare and Institutions Code sections 10850 and 14100.2, or 42 Code of Federal Regulations (CFR) section 431.300 et.seq, and 45 CFR 205.50 et.seq, or as required by law. Disclosures which are required by law, such as a court order, or which are made with the explicit written authorization of the client, are allowable. Any other use or disclosure of requires the express approval in writing of the COUNTY. Binti shall not duplicate, disseminate or disclose PII except as allowed in this Agreement.

3. Binti agrees to the PII Privacy and Security Standards attached as Attachment III. When applicable, Binti shall incorporate the relevant provisions of Attachment III into each subcontract or sub-award to subcontractors.

6. Term and Termination.

(a) Term. This Agreement will commence on the Effective Date and continue for a period of five (5) years **through June 30, 2027** ("**Initial Term**").

(b) Termination. Licensee may terminate this Agreement for any or no reason (in its sole and absolute discretion), upon thirty (30) days' written notice to Binti. Binti may terminate this Agreement for any or no reason (in its sole and

absolute discretion), upon ninety (90) days' written notice to Licensee. Either Party may terminate this Agreement upon thirty (30) days' prior written notice if the other Party is in material breach of this Agreement and the breaching Party fails to remedy such material breach within the thirty (30)-day notice period. Upon termination (except for termination by Binti pursuant to the immediately preceding sentence), the Licensee will have access to the Platform for the remainder of the then-current Term. Upon termination by either party for any reason, Binti will supply the Licensee with an export of the Licensee's Data.

(c) Effect of Termination. Upon expiration or termination of this Agreement for any reason, the licenses granted by each Party will automatically terminate and, except for Licensee's termination for Binti's uncured material breach, all outstanding Fees owed pursuant to Section 4 will become immediately due and payable. In the case of Licensee's termination for Binti's uncured material breach, Binti shall refund to Licensee any prepaid, but unearned fees for the period subsequent to the termination date. The provisions of Sections 1(b), 1(c), 2(b), 3(b), 4, 5, 6(c), 7, 8, 9, 10 and all defined terms used in those Sections will survive any expiration or termination of this Agreement.

7. Representations and Warranties.

(a) Mutual. Each Party represents and warrants that: (i) it has the right, power and authority to enter into this Agreement and to grant the rights and licenses granted hereunder and to perform all of its obligations hereunder; (ii) the execution of this Agreement by its representative whose signature is set forth at the end hereof has been duly authorized by all necessary organizational action of the Party; and (iii) when executed and delivered by both Parties, this Agreement will constitute the legal, valid and binding obligation of such Party, enforceable against such Party in accordance with its terms.

(b) Licensee. Licensee further represents and warrants that: (i) it owns or otherwise has sufficient rights to the Data to grant the license set forth in Section 1(d); and (ii) no Data submitted to the Platform does or will violate the privacy, intellectual property or other rights of any person or entity or any applicable laws, rules or regulations.

(c) EXCEPT FOR THE REPRESENTATIONS AND WARRANTIES SET FORTH UNDER THIS SECTION 7, THE SERVICES AND ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT BY BINTI ARE PROVIDED ON AN "AS-IS" BASIS, AND LICENSEE ASSUMES ALL RESPONSIBILITIES FOR THE ACCURACY AND/OR QUALITY OF ITS DATA, AND FOR ITS USE OF, AND RESULTS OBTAINED FROM, THE SERVICES. BINTI DOES NOT WARRANT THAT THE SERVICES OR ANYTHING ELSE PROVIDED IN CONNECTION WITH THIS AGREEMENT WILL BE ERROR-FREE OR THAT THE SERVICES WILL WORK WITHOUT INTERRUPTIONS. BINTI MAKES NO PROMISES, REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THE SERVICES, AND BINTI HEREBY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, AS WELL AS ANY LOCAL JURISDICTIONAL ANALOGUES TO THE FOREGOING.

8. Limitations on Liability. TO THE FULLEST EXTENT PERMITTED UNDER APPLICABLE LAW, (I) IN NO EVENT WILL EITHER PARTY'S TOTAL LIABILITY TO THE OTHER PARTY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED ONE MILLION NINE HUNDRED AND EIGHT THOUSAND DOLLARS (US\$1,908,000); AND (II) EXCEPT TO THE EXTENT SUCH DAMAGES ARE PAID OR PAYABLE TO UNAFFILIATED THIRD PARTIES PURSUANT TO EITHER PARTY'S OBLIGATIONS PURSUANT TO SECTION 9, IN NO EVENT WILL EITHER PARTY HAVE ANY LIABILITY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT (INCLUDING, WITHOUT LIMITATION, FOR LOST PROFITS, DATA OR OTHER BUSINESS OPPORTUNITIES), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE.

9. Indemnification.

(a) Licensee. Licensee agrees and acknowledges that Binti bears no responsibility or liability alleging or arising from any third party claim (a) that any Data infringes, violates, or misappropriates any intellectual property or proprietary right(s), (b) that any Data, or its provision to Binti, violates any applicable law or regulation, or (c) any negligent act or intentional misconduct by Licensee or any of its Authorized Users in connection with the Service.

(b) Binti. If a Third Party Claim is asserted against Licensee or any of its affiliates, officers, employees or contractors (each, a "Licensee Released Party") alleging that the Platform (not including any Data) infringes, violates, or misappropriates such third party's intellectual property or proprietary right(s) ("Infringement Claim"), then Binti will defend the Licensee Released Party from the Infringement Claim and hold such Party harmless from and against all damages, settlements, costs, and/or expenses, in each case, that are paid or payable with respect to the Infringement Claim (including, without limitation, reasonable attorneys' fees). In the event of an Infringement Claim, Binti, at its sole option and expense, may: (i) procure for Licensee the right to continue using the Platform or infringing part thereof; (ii) modify

the Platform or infringing part thereof; (iii) replace the Platform or infringing part thereof with other software having substantially the same or better capabilities; or, (iv) if the foregoing are not commercially practicable, terminate this Agreement and repay to Licensee a pro-rata portion of the Fees. Notwithstanding the foregoing sentences of this Section 9(b), Binti will have no liability for an Infringement Claim if the actual or alleged infringement results from (a) any breach of this Agreement by Licensee or any Authorized Users; (b) any modification, alteration or addition made to the Platform by Licensee or any Authorized Users, including any combination of the Platform with software not provided by Binti; (c) any failure by Licensee or any Authorized Users to use any Updates made available by Binti.

(c) Procedures. If a credible Infringement Claim is made or threatened, including without limitation the filing of a lawsuit against Licensee, or Licensee receives a demand or notice of an Infringement Claim claiming actual or potential infringement or misappropriation of any intellectual property rights, Licensee will use reasonable efforts to notify Binti promptly of such Infringement Claim. However, Licensee's failure to provide or delay in providing such notice will relieve Binti of its obligations only if and to the extent that such delay or failure materially prejudices Binti's ability to defend such Infringement Claim. Licensee will give Binti sole control of the defense and settlement of such Infringement Claim; provided that Binti may not settle the Infringement Claim absent the written consent of Licensee unless such settlement (a) includes a release of all Infringement Claims pending against Licensee, (b) contains no admission of liability or wrongdoing by Licensee, and (c) imposes no obligations upon Licensee other than an obligation to stop using the Platform and/or the payment of money (which is entirely covered by an indemnification obligation hereunder from Binti).

10. Insurance. Binti agrees to provide insurance in accordance with the requirements set forth in Attachment 1 hereto.

11. Miscellaneous. Each Party agrees that any violation or threatened violation of this Agreement may cause irreparable injury to the other Party, entitling such Party to seek injunctive relief in addition to all available remedies. Neither Party may assign this Agreement or any rights under it, in whole or in part, without the other Party's prior written consent; provided, however, that in the case of a sale of all or substantially all of the assets or business of Binti to which this Agreement relates, including by means of an acquisition, merger, or divestiture, Binti will notify Licensee as soon as reasonably possible, and provide Licensee with a copy of such assignment. Any attempt to assign this Agreement other than as permitted above will be void. If any provision of this Agreement is held by a court of competent jurisdiction to be unenforceable, then the remaining provisions of this Agreement will remain in full force and effect. This Agreement will be governed by and construed under the laws of California without reference to its conflict of laws principles. The parties acknowledge and agree that this Agreement is entered into and intended to be performed in Riverside County, California. The parties agree that the venue of any action or claim brought by any party to this Agreement will be the Superior Court of California, County of Riverside, Riverside District. Each party hereby waives any law or rule of the court, which would allow them to request or demand a change of venue. If any action or claim concerning this Agreement is brought by any third party and filed in another venue, the parties hereto agree to use their best efforts to obtain a change of venue to the Superior Court of California, County of Riverside, Riverside District. The parties shall attempt to resolve any disputes amicably at the working level. If that is not successful, the dispute shall be referred to the senior management of the parties. Binti shall proceed diligently with the performance of this Agreement pending resolution of a dispute. Prior to the filing of any legal action related to this Agreement, the parties shall be obligated to attend a mediation session in Riverside County before a neutral third-party mediator. A second mediation session shall be required if the first session is not successful. The parties shall share the cost of the mediations. This Agreement, including all Exhibits attached hereto, embodies the entire agreement between the Parties with respect to the subject matter set forth herein and supersedes any previous or contemporaneous communications, whether oral or written, express or implied. This Agreement may be modified or amended only by a writing signed by both Parties. If there is any conflict or inconsistency between the terms of any Exhibit and the terms in the body of this Agreement, then the terms in the body of the Agreement will control solely to the extent of the conflict. All waivers made under this Agreement must be made in writing by the Party making the waiver. Any notice required or permitted to be given under this Agreement will be effective if it is (i) in writing and sent by certified or registered mail, or insured courier, return receipt requested, to the appropriate Party at the address set forth above and with the appropriate postage affixed; or (ii) sent via email to the following: in the case of Binti: contract-notices@binti.com; and in the case of Licensee: Bridgette Hernandez - blhernan@rivco.org. Either Party may change its address for receipt of notice by notice to the other Party in accordance with this Section. Notices are deemed given two (2) business days following the date of mailing, one (1) business day following delivery to a courier, and/or on the first business day after a facsimile or electronic mail is sent to the recipient with confirmation of receipt. Binti will not be liable or responsible to Licensee, nor be deemed to have breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement when and to the extent such failure or delay is caused by or results from acts or circumstances beyond the reasonable control of Binti including, without limitation, acts of God, natural disaster, denial or services attacks and/or service provider system outages (collectively, "**Force Majeure Events**"). This Agreement may be executed in any number of counterparts, each of which so executed shall be deemed to be an original, and such counterparts shall together constitute one and the same Agreement. The parties shall be entitled to sign and transmit an electronic signature of this Agreement (whether by facsimile, PDF or other email transmission), which signature shall be binding on

the party whose name is contained therein. Each party providing an electronic signature agrees to promptly execute and deliver to the other party an original signed Agreement upon request.

BINTI, INC.

LICENSEE

Authorized Signature for Binti, Inc. <i>Felicia Curcuru</i>	Authorized Signature for County <i>Jeff Hewitt</i>
Printed Name of Person Signing: Felicia Curcuru	Printed Name of Person Signing: Jeff Hewitt
Title: Chief Executive Officer	Title: Chairman of the Board
Date Signed: Nov 17, 2022	Date Signed: Dec 6, 2022

Approval as to Form
Minh Tran
County Counsel

By: *Katherine Wilkins*
Katherine Wilkins
Deputy County Counsel
Date: Nov 17, 2022



ATTEST:
KECIA R. HARPER, Clerk
By: *Cindy Fernandez*
DEPUTY

EXHIBIT A

PROFESSIONAL SERVICES

All capitalized terms that are used but not defined in this Exhibit will have the meanings ascribed to them in the body of the Agreement above.

1. Contact. The principal contacts in connection with the Professional Services are as follows:

Binti:	Licensee:
Name: Veronica Davis	Name: Bridgette Hernandez
Title: Head of Project Management Organization	Title: Deputy Director
Address: 1212 Broadway, Suite 200, Oakland, California 94612	Address: 4060 County Circle Dr., Riverside, CA 92503
Phone: 844-424-6844	Phone: 951-358-3115
Email: pmo @binti.com	Email: blhernan@rivco.org

2. Implementation. All deliverables will be reviewed and accepted by the assigned COUNTY-DPSS Project Manager. Each party's responsibilities and the project deliverables are listed in the following table:

- a. Milestones.

Milestone #1 – Participate in kick-off call, develop a project plan, identify key persons from County for key launch components; provide training resources.		
CONTRACTOR RESPONSIBILITIES	COUNTY-DPSS RESPONSIBILITIES	DELIVERABLES
Schedule and facilitate the initial "Kick-Off" meeting.	Participate in a "Kick-Off" meeting conducted virtually through MS TEAMS. Provide the Contractor with access to the MS TEAMS meeting	Completion of the Kick-Off meeting
Develop and submit a project timeline and plan.	Provide the Contractor with access to necessary resources and documentation.	A Project Plan laying out the key deliverables and milestones for completion of the project to include: System Migration Strategy that identifies the best approach for implementation and rollout. Project Work Plan that identifies deliverables, resources, task dependencies, and work schedule of the project.
Provide access to training resources		Binti Help Center, recorded trainings, and access to Binti subject matter experts.
MILESTONE #2 – Placements Module is launched, and data imported - Includes training		

CONTRACTOR RESPONSIBILITIES	COUNTY-DPSS RESPONSIBILITIES	DELIVERABLES
Collect all relevant placement forms, complete three template walk through meetings for the placement template	Provide placement forms to Contractor. Participate in walk through meetings and provide feedback.	Incorporate placement forms into Binti platform. Walk through forms with County to confirm accuracy.
Complete import of historical data related to placements (such as child and placement period data)	Complete a value-mapping exercise. Provide placements data in accordance with import template	Data import is completed
Activation of the Placements Module		Placements Module is live
Be responsible for training business administrators, end users, and County trainers (train-the-trainer).	Be responsible for scheduling and staff attendance.	Delivery of: Training Curriculum that identifies the approach, type of training, course outlines and objectives, and course schedules. Completion of training.
MILESTONE #3 – Health Check 1 (30 days after the launch of the Placements Module)		
CONTRACTOR RESPONSIBILITIES	COUNTY-DPSS RESPONSIBILITIES	DELIVERABLES
Provide health check-in to get feedback, provide recommendations, and support agency success.	Attend health check and provide feedback and recommendations to Binti Customer Success Manager	Health Check 2 meeting has taken place
MILESTONE #4 – Website Built		
CONTRACTOR RESPONSIBILITIES	COUNTY-DPSS RESPONSIBILITIES	DELIVERABLES
Design and build a 4-page website to support recruitment efforts	Provide all written and visual content Review and accept website before go-live	Recruiting website is live
Milestone #5 – Collect RFA Forms and begin the walkthrough process. Begin data import process		
CONTRACTOR RESPONSIBILITIES	COUNTY-DPSS RESPONSIBILITIES	DELIVERABLES
Develop data Migration Plan to analyze the data for gaps and identify issues.	Complete a value-mapping exercise with the Contractor. Provide data to the Contractor.	Provide data Migration plan and instructions
Begin to migrate data as defined in the data migration plan and conduct conformance testing.	Conduct User Acceptance Testing.	Contractor test results and User Acceptance test results.
Collect all relevant RFA forms, complete three template walk through meetings for the RFA template	Provide RFA forms to Contractor. Participate in walk through meetings and provide feedback.	Incorporate RFA forms into Binti platform. Walk through forms with County to confirm accuracy.
MILESTONE #6– Grievances functionality and Exemptions Functionality - RFA Module		

CONTRACTOR RESPONSIBILITIES	COUNTY-DPSS RESPONSIBILITIES	DELIVERABLES
<p>Develop Grievance functionality with the RFA module that will allow agency workers to:</p> <ul style="list-style-type: none"> Allow indication that a family/applicant has filed a grievance Track the status of the grievance and key milestones Allow for agency staff to store required grievance paperwork and documentation within Binti Develop <p>Exemption functionality within the RFA module that will allow agency workers to:</p> <ul style="list-style-type: none"> Collect data based on certain crime types, in addition to the race and annual income of the person with the exemption via a drop down. Allow staff to indicate exemptions required by background check Display on the application dashboard which applicants require exemptions On the background check exemptions page, indicate which specific background checks require exemptions For each background check that requires exemptions, allow staff to indicate/display the type of exemption required (such as standard, simplified, SB 354, etc.) and the overall status of that background check exemption (such as pending, approved, denied, etc.) For each background check that requires exemptions, allow agency staff to track timelines of when required processes are carried out, such as completion of required documentation and approval/non-approval by caseworker/supervisor/manager/deputy/assistant director Within the background check log, ability to see all background checks logged and filtered by date, caseworker, or applicant, as well as a log of those that required exemptions and current status (pending, granted, etc.) 	<p>Participate in at least eight (8), 1-hour user sessions to share workflow processes related to grievances and exemptions</p> <p>Provide feedback on functionality development</p>	<p>Grievance and exemption functionality developed and deployed into the RFA module as described in the Contractor Responsibilities section of this Milestone</p>

Milestone #7 - RFA Module is live - allowing data to flow into Placements, training for RFA staff		
CONTRACTOR RESPONSIBILITIES	COUNTY-DPSS RESPONSIBILITIES	DELIVERABLES
Be responsible for the configuration of the RFA Module.	Provide all requirements for configuration to Binti in a timely fashion	RFA approval module goes live.
Be responsible for training business administrators, end users, and County trainers (train-the-trainer).	Be responsible for scheduling and staff attendance.	Delivery of: Training Curriculum that identifies the approach, type of training, course outlines and objectives, and course schedules. Completion of training.
MILESTONE #8 – Health Check 2 (30 days after RFA Implementation)		
CONTRACTOR RESPONSIBILITIES	COUNTY-DPSS RESPONSIBILITIES	DELIVERABLES
Provide health check-in to get feedback, provide recommendations, and support agency success.	Attend health check and provide feedback and recommendations to Binti Customer Success Manager	Health Check 1 meeting has taken place

3. Acceptance of Deliverables.

- a. All deliverables will be reviewed and accepted by the assigned DPSS Project manager.
- b. CONTRACTOR will notify the DPSS Project Manager via email of the completion of each deliverable(s). DPSS shall have a period of five (5) business days from receipt of notification to determine the acceptability of a deliverable provided by CONTRACTOR hereunder (the “Acceptance Period”).
- c. At any time within the acceptance period, DPSS shall:
 - i. Provide written approval with a reply via email or;
 - ii. Provide written notice of non-acceptance (as determined in DPSS’s reasonable discretion) with reasonable written comments to CONTRACTOR regarding the deficiencies of the deliverable(s). If changes or modifications are required by DPSS as evidenced by the non-acceptance notification, CONTRACTOR shall have ten (10) business days to correct the deficiency noted therein and/or submit a plan for correction of such deficiencies which shall be reasonably acceptable to both parties. This process shall not exceed two cycles.
- d. All Deliverables will be delivered either electronically or in paper form to the County in English, unless otherwise specified in the Statement of Work. The County will deliver to Contractor all documents, studies, and materials in English, unless otherwise specified in the Statement of Work. All electronic documents will use the Microsoft suite of products, including, but not limited to Word, Excel, PowerPoint, Project, and Visio Pro. Signature pages may be delivered using Adobe PDF.
- e. The County will be deemed to have accepted the Deliverable(s) upon occurrence of either of the following (“Acceptance”):
 - i. The County submits to the Contractor approval via email or;
 - ii. The County fails to notify Contractor within the Acceptance Period described above.

4. Services. Binti will use commercially reasonable efforts to provide the following Professional Services:

- a. Data Migration. Migrate Data into the Platform based on reasonably written instructions from Licensee within 12 weeks of receiving data with documentation from Licensee.

- b. Form Customizations. Customize up to 60 documents provided to Binti by Licensee for inclusion within the Platform within 12 weeks of Licensee providing the documents.
- c. Web Development: Develop custom public facing website with specifications agreed upon between Licensee and Binti within 4 weeks of Licensee providing requested information from Binti.
- d. Any additional Professional Services to be performed by Binti will be mutually agreed upon by the Parties in writing and attached to this Exhibit A as successively numbered Schedule "A"s (*e.g.*, Schedule A-1, Schedule A-2, etc.).

This Exhibit A is accepted and agreed upon as of the Effective Date set forth in the body of the Agreement.

EXHIBIT B

SUPPORT

All capitalized terms that are used but not defined in this Exhibit will have the meanings ascribed to them in the body of the Agreement above.

1. **Support.** Binti will provide technical support to Licensee from 6AM-6PM Pacific Standard time Monday through Friday during the Term except for national holidays in the United States and June 19th. Support may be non-live and/or limited for up to four (4) days per year due to staff training. ("**Support**"). To request Support, Licensee must contact Binti via Live Chat within family.binti.com, via phone at 844-424-6844, or via email at help@binti.com. Support will return/answer all messages received outside of the aforementioned hours during the following business day.

(a) **Provision of Support.** Binti will provide Support to the following Licensee contact: **see Exhibit A, Licensee.** Binti will not be responsible for addressing or resolving Events (defined below) that Binti reasonably determines are caused by Licensee's systems or any misuse of the Platform.

(b) **Events.** "**Events**" are occurrences that impact the availability of the Platform, except for scheduled downtime, as determined by Binti in its reasonable discretion. Binti distinguishes among three classes of Events as follows:

- (i) **Critical Event:** A complete loss of the Platform's functionality such that no user can use the Platform.
- (ii) **High Event:** The Platform's functionality is materially impaired such that at least approximately 10% of users cannot use the Platform for its intended purpose. Users have major impact and minimal functionality is available.
- (iii) **Medium Event:** An event not meeting the criteria of Critical or High, has a workaround available, which does not negatively impact the User from using the Platform for its intended purpose. Such errors will be consistent and reproducible. Users would lose some level of functionality but are still able to utilize the system.
- (iv) **Low Event:** Any other problems or issues, without limitation, any general questions about the Platform or problems that do not rise to Critical, High, or Medium events. Most users would not notice or be impacted if not addressed.

(c) **Target Resolution Times.** Binti will use commercially reasonable efforts to meet the following target time frames for resolution of Events from the time Binti receives a Support request:

Event Level	Target Resolution Time
Critical	4 hours or better
High	24 hours or better
Medium Low	Binti will provide a response time of 3 business days; resolution will be determined based on an agreed action/remediation plan between the Parties in writing

(d) **Scheduled Maintenance Downtime.** Binti will schedule maintenance between the hours of 10PM and 4AM Pacific Standard time. Binti will provide Licensee with reasonable advance written notice of scheduled downtime. Binti may access the Platform during the scheduled maintenance downtimes for maintenance purposes and to implement Updates, bug fixes and/or any other changes that Binti deems necessary or advisable. Outside of scheduled maintenance downtime, Binti maintains a 99.5% system uptime.

(e) **Resolution.** If Binti has not resolved an Event within the targeted time frame, then, upon Licensee's written request, Binti and Licensee will discuss a resolution plan. From that point forward until the issue is resolved, Binti will notify Licensee's designated contact of the status of resolution at least once daily.

2. **Training.** The Parties may agree in writing upon commercially reasonable training that Binti will provide to Licensee Authorized Users during the Term. This may include, by way of example only, a web-based tutorial about how to use the Platform. Training will not exceed a total of 25 hours during the Term.

ATTACHMENT I
INSURANCE REQUIREMENTS

Binti agrees to provide insurance set forth in accordance with the requirements herein. If Binti uses existing coverage to comply with these requirements and that coverage does not meet the specified requirements, Binti agrees to amend, supplement or endorse the existing coverage to do so.

1. INSURANCE

- a. Without limiting or diminishing the CONTRACTOR'S obligation to indemnify or hold the COUNTY harmless, CONTRACTOR shall procure and maintain or cause to be maintained, at its sole cost and expense, the following insurance coverage's during the term of this Agreement. As respects to the insurance section only, the COUNTY herein refers to the County of Riverside, its Agencies, Districts, Special Districts, and Departments, their respective directors, officers, Board of Supervisors, employees, elected or appointed officials, agents or representatives as Additional Insureds.
- b. Any insurance carrier providing insurance coverage hereunder shall be admitted to the State of California and have an AM BEST rating of not less than A: VIII (A:8) unless such requirements are waived, in writing, by the County Risk Manager. If the County's Risk Manager waives a requirement for a particular insurer such waiver is only valid for that specific insurer and only for one policy term.
- c. CONTRACTOR's insurance carrier(s) must declare its insurance self-insured retentions. If such self-insured retentions exceed \$500,000 per occurrence such retentions shall have the prior written consent of the County Risk Manager before the commencement of operations under this Agreement. Upon notification of self-insured retention unacceptable to COUNTY, and at the election of the County's Risk Manager, CONTRACTOR's carriers shall either; 1) reduce or eliminate such self-insured retention as respects to this Agreement with COUNTY, or 2) procure a bond which guarantees payment of losses and related investigations, claims administration, and defense costs and expenses.
- d. CONTRACTOR shall cause CONTRACTOR's insurance carrier(s) to furnish the COUNTY with either 1) a properly executed original certificate(s) of insurance and certified original copies of endorsements effecting coverage as required herein, or 2) if requested to do so orally or in writing by the County Risk Manager, provide original certified copies of policies, including all endorsements and all attachments thereto, showing such insurance is in full force and effect. Further, said Certificate(s) and policies of insurance shall contain the covenant of the insurance carrier(s) that thirty (30) calendar days written notice shall be given to the COUNTY prior to any material modification, cancellation, expiration or reduction in coverage of such insurance. In the event of a material modification, cancellation, expiration, or reduction in coverage, this Agreement shall terminate forthwith, unless the COUNTY receives, prior to such effective date, another properly executed original Certificate of Insurance and original copies of endorsements or certified original policies, including all endorsements and attachments thereto evidencing coverages set forth herein and the insurance required herein is in full force and effect. CONTRACTOR shall not commence operations until the COUNTY has been furnished original certificate(s) of insurance and certified original copies of endorsements and if requested, certified original policies of insurance including all endorsements and any and all other attachments as required in this section. An individual authorized by the insurance carrier to do so on its behalf shall sign the original endorsements for each policy and the certificate of insurance.
- e. It is understood and agreed to by the parties hereto that CONTRACTOR's insurance shall be construed as primary insurance, and COUNTY's insurance and/or deductibles and/or self-insured retentions or self-insured programs shall not be construed as contributory.
- f. If, during the term of this Agreement or any extension thereof, there is a material change in the scope of services, or there is a material change in the equipment to be used in the performance of the scope of work which will add additional exposures (such as the use of aircraft, watercraft, cranes, etc.), or the term of this Agreement, including any extensions thereof, exceeds five (5) years, the COUNTY reserves the right to adjust the types of insurance required under this Agreement and the monetary limits of liability for the insurance coverages currently required herein if, in the County Risk Manager's reasonable judgment, the amount or type of insurance carried by the CONTRACTOR has become inadequate.

- g. CONTRACTOR shall pass down the insurance obligations contained herein to all tiers of subcontractors working under this Agreement.
- h. The insurance requirements contained in this Agreement may be met with a program(s) of self-insurance acceptable to COUNTY.
- i. CONTRACTOR agrees to notify COUNTY of any claim by a third party or any incident or event that may give rise to a claim arising from the performance of this Agreement.

2. WORKER'S COMPENSATION

If the CONTRACTOR has employees as defined by the State of California, the CONTRACTOR shall maintain statutory Workers' Compensation Insurance (Coverage A) as prescribed by the laws of the State of California. Policy shall include Employers' Liability (Coverage B) including Occupational Disease with limits not less than \$1,000,000 per person per accident. The policy shall be endorsed to waive subrogation in favor of The County of Riverside.

3. VEHICLE LIABILITY

If vehicles or mobile equipment are used in the performance of the obligations under this Agreement, then CONTRACTOR shall maintain liability insurance for all owned, non-owned or hired vehicles so used in an amount not less than \$1,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this agreement or be no less than two (2) times the occurrence limit. Policy shall name the COUNTY as Additional Insureds.

4. COMMERCIAL GENERAL LIABILITY

Commercial General Liability insurance coverage, including but not limited to, premises liability, unmodified contractual liability, products and completed operations liability, personal and advertising injury, and cross liability coverage, covering claims which may arise from or out of CONTRACTOR'S performance of its obligations hereunder. Policy shall name the COUNTY as Additional Insured. Policy's limit of liability shall not be less than \$2,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this agreement or be no less than two (2) times the occurrence limit.

5. CYBER LIABILITY

CONTRACTOR shall procure and maintain for the duration of the contract insurance against claims for injuries to person or damages to property which may arise from or in connection with the performance of the work hereunder by CONTRACTOR, its agents, representatives, or employees. CONTRACTOR shall procure and maintain for the duration of the contract insurance claims arising out of their services and including, but not limited to loss, damage, theft or other misuse of data, infringement of intellectual property, invasion of privacy and breach of data.

CONTRACTOR shall procure and maintain cyber liability Insurance, with limits not less than \$2,000,000 per occurrence or claim, \$2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by CONTRACTOR in this Agreement and shall include, but not limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

If CONTRACTOR maintains broader coverage and/or higher limits than the minimums shown above, COUNTY requires and shall be entitled to the broader coverage and/or higher limits maintained by CONTRACTOR. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to COUNTY.

**ATTACHMENT II
FISCAL PROVISIONS**

A. MAXIMUM REIMBURSABLE AMOUNT

The maximum reimbursable amount of this agreement shall not exceed the amounts indicated in the table below over the period of five (5) years.

Product	During Initial Implementation (as defined at the ** below)	After Full Implementation*** through June 30, 2027
Binti Saas for Placements/Matching Module, Binti Saas for RFA Approvals Module, Binti Public Recruiting Website (see note on Public Recruiting Website below)	\$250,000	\$463,000 annually
Total	\$250,000 (“Baseline Fee”)	\$463,000 annually (“Full Fee”)

**“Initial Implementation” shall refer to the completion of the items set forth in Milestones 1 through 8 set forth in Section B below. During the Initial Implementation (as defined in Exhibit A, Attachment II) phase, upon the “Acceptance” (as defined in Exhibit A, 2(a)) of each Milestone (as set forth in Exhibit A, Attachment II, Section B), Licensee will pay Binti the corresponding payment amount as set forth therein. At “Full Implementation” (as defined in Attachment II) of all milestones as set forth in Section 2(a) of Exhibit A hereto, Licensee will pay Binti a pro-rated annual fee for the remainder of the then current fiscal year in advance calculated as follows: divide the number of days remaining in the then current fiscal year (which begins on July 1st and ends on June 30th) by 365 days, then multiply that percentage by \$463,000. After full implementation, the annual full fee may be increased up to 5% annually, subject to Binti and DPSS approval, by way of written amendment. By request of DPSS in connection with enhancements and/or improvements made to the Platform or Professional Services, Binti may increase the Fees by an amount deemed necessary by Binti, subject to DPSS’ approval upon sixty (60) days prior written notice. Any changes to fees must be made by way of written amendment. Subject to the preceding sentence, thereafter, in advance of each subsequent fiscal year through June 30, 2027, Binti will be paid \$463,000 for access to the RFA Approvals Module, Placement/Matching Module and Public Recruiting Website.

*****This is an annual licensing fee which includes:**

- The license of the RFA/Approvals and Placements/Matching software for all resource family applicants and social workers;
- Training for agency workers both upfront and ongoing;
- Import of historic data;
- Configuration of all forms (both upfront and if/when forms change);
- Monthly check-ins to get feedback and make sure things are going well;
- Ongoing feature improvements and fixing any issues;
- Unlimited number of users;
- Customer support (through email, phone and live chat in English and in Spanish); and
- Use of Binti’s API: Binti’s Application Programming Interface (API) is available to agencies as a method to programmatically connect systems for performing a secure data exchange. The Binti API provides access to agency data as defined by the core Binti data model.
 - o Binti has specific endpoints within our API available for data integration, as described here: <https://family.binti.com/api-docs/index.html>. Technical documentation is available upon request to provide additional information.
 - o Any additional set-up/configuration with regards to Binti’s API (if any) for County shall be discussed and agreed upon by both parties, and then would be described in Exhibit B (Professional Services)

B. PAYMENT SCHEDULE FOR IMPLEMENTATION

Milestone Description	Payment
MILESTONE #1 – Participate in kick-off call; develop a project plan; identify key persons from County for key launch components; develop first draft of training material and documentation.	\$40,000
MILESTONE #2 – Launch Placements module - Data is imported and training is provided, and Placements module is turned on/available for users	\$130,000
MILESTONE #3 – Health Check 1 conducted by the Binti team to get feedback, provide recommendations, and support agency success at 30 days after Placements launch	\$5,000
MILESTONE #4 – Website Built	\$10,000
Milestone #6 – Collect all RFA related forms; Complete three template walk through meetings for the RFA template; begin data import process (data import does not need to be complete to trigger milestone payment).	\$20,000
MILESTONE #5– Grievances & Exemptions as part of full RFA module package	\$213,000
Milestone #7 - Launch RFA module (meaning County is live in a production site, County staff have been trained, and County data is live in Binti (or there is a plan for making it live in Binti) (“Implementation”)	\$40,000
MILESTONE #8 – Health Check 2 conducted by the Binti team, to get feedback, provide recommendations, and support agency success at 30 days after RFA implementation	\$5,000
TOTAL REIMBURSABLE AMOUNT	\$463,000

C. Invoices and fiscal related documents shall be submitted via email to: ClientServicesContracts@rivco.org

D. METHOD, TIME, AND CONDITIONS OF PAYMENT

1. Binti will be paid the actual amount of each approved invoice. Licensee may delay payment if the required supporting documentation is not provided. During implementation, each invoice must include Licensee’s approval of milestone acceptance pursuant to Exhibit A, section 3.

E. The Licensee is not responsible for any fees or costs incurred above or beyond the contracted amount and shall have no obligation to purchase any specified amount of services or products.

ATTACHMENT III
HIPAA Business Associate Agreement
Addendum to Contract
Between the County of Riverside and Unassigned

This HIPAA Business Associate Agreement (the "Addendum") supplements, and is made part of (the DPSS-0004647 "Underlying Agreement") between the County of Riverside ("County") and Binti, Inc. ("Contractor") and shall be effective as of the date the Underlying Agreement is approved by both Parties (the "Effective Date").

RECITALS

WHEREAS, County and Contractor entered into the Underlying Agreement pursuant to which the Contractor provides services to County, and in conjunction with the provision of such services certain protected health information ("PHI") and/or certain electronic protected health information ("ePHI") may be created by or made available to Contractor for the purposes of carrying out its obligations under the Underlying Agreement; and,

WHEREAS, the provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191 enacted August 21, 1996, and the Health Information Technology for Economic and Clinical Health Act ("HITECH") of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 enacted February 17, 2009, and the laws and regulations promulgated subsequent thereto, as may be amended from time to time, are applicable to the protection of any use or disclosure of PHI and/or ePHI pursuant to the Underlying Agreement; and,

WHEREAS, County is a covered entity, as defined in the Privacy Rule; and,

WHEREAS, to the extent County discloses PHI and/or ePHI to Contractor or Contractor creates, receives, maintains, transmits, or has access to PHI and/or ePHI of County, Contractor is a business associate, as defined in the Privacy Rule; and,

WHEREAS, pursuant to 42 USC §17931 and §17934, certain provisions of the Security Rule and Privacy Rule apply to a business associate of a covered entity in the same manner that they apply to the covered entity, the additional security and privacy requirements of HITECH are applicable to business associates and must be incorporated into the business associate agreement, and a business associate is liable for civil and criminal penalties for failure to comply with these security and/or privacy provisions; and,

WHEREAS, the parties mutually agree that any use or disclosure of PHI and/or ePHI must be in compliance with the Privacy Rule, Security Rule, HIPAA, HITECH and any other applicable law; and,

WHEREAS, the parties intend to enter into this Addendum to address the requirements and obligations set forth in the Privacy Rule, Security Rule, HITECH and HIPAA as they apply to Contractor as a business associate of County, including the establishment of permitted and required uses and disclosures of PHI and/or ePHI created or received by Contractor during the course of performing functions, services and activities on behalf of County, and appropriate limitations and conditions on such uses and disclosures;

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

1. **Definitions.** Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in HITECH, HIPAA, Security Rule and/or Privacy Rule, as may be amended from time to time.
 - A. "Breach" when used in connection with PHI means the acquisition, access, use or disclosure of PHI in a manner not permitted under subpart E of the Privacy Rule which compromises the security or privacy of the PHI, and shall have the meaning given such term in 45 CFR §164.402.
 - (1) Except as provided below in Paragraph (2) of this definition, acquisition, access, use, or disclosure of PHI in a manner not permitted by subpart E of the Privacy Rule is presumed to be a breach unless Contractor demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors:
 - (a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
 - (b) The unauthorized person who used the PHI or to whom the disclosure was made;
 - (c) Whether the PHI was actually acquired or viewed; and
 - (d) The extent to which the risk to the PHI has been mitigated.
 - (2) Breach excludes:
 - (a) Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of the Privacy Rule.
 - (b) Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement in which County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by subpart E of the Privacy Rule.
 - (c) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
 - B. "Business associate" has the meaning given such term in 45 CFR §164.501, including but not limited to a subcontractor that creates, receives, maintains, transmits or accesses PHI on behalf of the business associate.
 - C. "Data aggregation" has the meaning given such term in 45 CFR §164.501.

- D. "Designated record set" as defined in 45 CFR §164.501 means a group of records maintained by or for a covered entity that may include: the medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or, used, in whole or in part, by or for the covered entity to make decisions about individuals.
- E. "Electronic protected health information" ("ePHI") as defined in 45 CFR §160.103 means protected health information transmitted by or maintained in electronic media.
- F. "Electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff, and shall have the meaning given such term in 42 USC §17921(5).
- G. "Health care operations" has the meaning given such term in 45 CFR §164.501.
- H. "Individual" as defined in 45 CFR §160.103 means the person who is the subject of protected health information.
- I. "Person" as defined in 45 CFR §160.103 means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.
- J. "Privacy Rule" means the HIPAA regulations codified at 45 CFR Parts 160 and 164, Subparts A 17 and E.
- K. "Protected health information" ("PHI") has the meaning given such term in 45 CFR §160.103, which includes ePHI.
- L. "Required by law" has the meaning given such term in 45 CFR §164.103.
- M. "Secretary" means the Secretary of the U.S. Department of Health and Human Services 22 ("HHS").
- N. "Security incident" as defined in 45 CFR §164.304 means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- O. "Security Rule" means the HIPAA Regulations codified at 45 CFR Parts 160 and 164, Subparts 27 A and C.
- P. "Subcontractor" as defined in 45 CFR §160.103 means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
- Q. "Unsecured protected health information" and "unsecured PHI" as defined in 45 CFR §164.402 means PHI not rendered unusable, unreadable, or indecipherable to unauthorized persons through use of a technology or methodology specified by the Secretary in the guidance issued 34 under 42 USC §17932(h)(2).

2. Scope of Use and Disclosure by Contractor of County's PHI and/or ePHI.

- A. Except as otherwise provided in this Addendum, Contractor may use, disclose, or access PHI and/or ePHI as necessary to perform any and all obligations of Contractor under the Underlying Agreement or to perform functions, activities or services for, or on behalf of, County as specified in this Addendum, if such use or disclosure does not violate HIPAA, HITECH, the Privacy Rule and/or Security Rule.
- B. Unless otherwise limited herein, in addition to any other uses and/or disclosures permitted or authorized by this Addendum or required by law, in accordance with 45 CFR §164.504(e)(2), Contractor may:
 - (1) Use PHI and/or ePHI if necessary for Contractor's proper management and administration and to carry out its legal responsibilities; and,
 - (2) Disclose PHI and/or ePHI for the purpose of Contractor's proper management and administration or to carry out its legal responsibilities, only if:
 - (a) The disclosure is required by law; or,
 - (b) Contractor obtains reasonable assurances, in writing, from the person to whom Contractor will Hold such PHI disclose such PHI and/or ePHI that the person will:
 - (i) and/or ePHI in confidence and use or further disclose it only for the purpose for which Contractor disclosed it to the person, or as required by law; and,
 - (ii) Notify Contractor of any instances of which it becomes aware in which the confidentiality of the information has been breached; and,
 - (3) Use PHI to provide data aggregation services relating to the health care operations of County pursuant to the Underlying Agreement or as requested by County; and,
 - (4) De-identify all PHI and/or ePHI of County received by Contractor under this Addendum provided that the de-identification conforms to the requirements of the Privacy Rule and/or 24 Security Rule and does not preclude timely payment and/or claims processing and receipt.
- C. Notwithstanding the foregoing, in any instance where applicable state and/or federal laws and/or regulations are more stringent in their requirements than the provisions of HIPAA, including, but not limited to, prohibiting disclosure of mental health and/or substance abuse records, the applicable state and/or federal laws and/or regulations shall control the disclosure of records.

3. Prohibited Uses and Disclosures.

- A. Contractor may neither use, disclose, nor access PHI and/or ePHI in a manner not authorized by the Underlying Agreement or this Addendum without patient authorization or de-identification of the PHI and/or ePHI and as authorized in writing from County.
- B. Contractor may neither use, disclose, nor access PHI and/or ePHI it receives from County or from another business associate of County, except as permitted or required by this Addendum, or as required by law.

- C. Contractor agrees not to make any disclosure of PHI and/or ePHI that County would be prohibited from making.
- D. Contractor shall not use or disclose PHI for any purpose prohibited by the Privacy Rule, Security Rule, HIPAA and/or HITECH, including, but not limited to 42 USC §17935 and §17936. Contractor agrees:
 - (1) Not to use or disclose PHI for fundraising, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.514(f) or 45 CFR §164.508;
 - (2) Not to use or disclose PHI for marketing, as defined in 45 CFR §164.501, unless pursuant to the Underlying Agreement and only if permitted by and in compliance with the requirements of 45 CFR §164.508(a)(3);
 - (3) Not to disclose PHI, except as otherwise required by law, to a health plan for purposes of carrying out payment or health care operations, if the individual has requested this restriction pursuant to 42 USC §17935(a) and 45 CFR §164.522, and has paid out of pocket in full for the health care item or service to which the PHI solely relates; and,
 - (4) Not to receive, directly or indirectly, remuneration in exchange for PHI, or engage in any act that would constitute a sale of PHI, as defined in 45 CFR §164.502(a)(5)(ii), unless permitted by the Underlying Agreement and in compliance with the requirements of a valid authorization under 45 CFR §164.508(a)(4). This prohibition shall not apply to payment by County to Contractor for services provided pursuant to the Underlying Agreement.

4. Obligations of County.

- A. County agrees to make its best efforts to notify Contractor promptly in writing of any restrictions on the use or disclosure of PHI and/or ePHI agreed to by County that may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.
- B. County agrees to make its best efforts to promptly notify Contractor in writing of any changes in, or revocation of, permission by any individual to use or disclose PHI and/or ePHI, if such changes or revocation may affect Contractor's ability to perform its obligations under the Underlying Agreement, or this Addendum.
- C. County agrees to make its best efforts to promptly notify Contractor in writing of any known limitation(s) in its notice of privacy practices to the extent that such limitation may affect Contractor's use or disclosure of PHI and/or ePHI.
- D. County agrees not to request Contractor to use or disclose PHI and/or ePHI in any manner that would not be permissible under HITECH, HIPAA, the Privacy Rule, and/or Security Rule.
- E. County agrees to obtain any authorizations necessary for the use or disclosure of PHI and/or ePHI, so that Contractor can perform its obligations under this Addendum and/or Underlying Agreement.

5. **Obligations of Contractor.** In connection with the use or disclosure of PHI and/or ePHI, Contractor agrees to:
- A. Use or disclose PHI only if such use or disclosure complies with each applicable requirement of 45 CFR §164.504(e). Contractor shall also comply with the additional privacy requirements that are applicable to covered entities in HITECH, as may be amended from time to time.
 - B. Not use or further disclose PHI and/or ePHI other than as permitted or required by this Addendum or as required by law. Contractor shall promptly notify County if Contractor is required by law to disclose PHI and/or ePHI.
 - C. Use appropriate safeguards and comply, where applicable, with the Security Rule with respect to ePHI, to prevent use or disclosure of PHI and/or ePHI other than as provided for by this Addendum.
 - D. Mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PHI and/or ePHI by Contractor in violation of this Addendum.
 - E. Report to County any use or disclosure of PHI and/or ePHI not provided for by this Addendum or otherwise in violation of HITECH, HIPAA, the Privacy Rule, and/or Security Rule of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410.
 - F. In accordance with 45 CFR §164.502(e)(1)(ii), require that any subcontractors that create, receive, maintain, transmit or access PHI on behalf of the Contractor agree through contract to the same restrictions and conditions that apply to Contractor with respect to such PHI and/or ePHI, including the restrictions and conditions pursuant to this Addendum.
 - G. Make available to County or the Secretary, in the time and manner designated by County or Secretary, Contractor's internal practices, books and records relating to the use, disclosure and privacy protection of PHI received from County, or created or received by Contractor on behalf of County, for purposes of determining, investigating or auditing Contractor's and/or County's compliance with the Privacy Rule.
 - H. Request, use or disclose only the minimum amount of PHI necessary to accomplish the intended purpose of the request, use or disclosure in accordance with 42 USC §17935(b) and 45 CFR §164.502(b)(1).
 - I. Comply with requirements of satisfactory assurances under 45 CFR §164.512 relating to notice or qualified protective order in response to a third party's subpoena, discovery request, or other lawful process for the disclosure of PHI, which Contractor shall promptly notify County upon Contractor's receipt of such request from a third party.
 - J. Not require an individual to provide patient authorization for use or disclosure of PHI as a condition for treatment, payment, enrollment in any health plan (including the health plan administered by County), or eligibility of benefits, unless otherwise excepted under 45 CFR §164.508(b)(4) and authorized in writing by County.
 - K. Use appropriate administrative, technical and physical safeguards to prevent inappropriate use, disclosure, or access of PHI and/or ePHI.

- L. Obtain and maintain knowledge of applicable laws and regulations related to HIPAA and HITECH, as may be amended from time to time.
- M. Comply with the requirements of the Privacy Rule that apply to the County to the extent Contractor is to carry out County's obligations under the Privacy Rule.
- N. Take reasonable steps to cure or end any pattern of activity or practice of its subcontractor of which Contractor becomes aware that constitute a material breach or violation of the subcontractor's obligations under the business associate contract with Contractor, and if such steps are unsuccessful, Contractor agrees to terminate its contract with the subcontractor if feasible.

6. Access to PHI, Amendment and Disclosure Accounting. Contractor agrees to:

- A. **Access to PHI, including ePHI.** Provide access to PHI, including ePHI if maintained electronically, in a designated record set to County or an individual as directed by County, within five (5) days of request from County, to satisfy the requirements of 45 CFR §164.524.
- B. **Amendment of PHI.** Make PHI available for amendment and incorporate amendments to PHI in a designated record set County directs or agrees to at the request of an individual, within fifteen (15) days of receiving a written request from County, in accordance with 45 CFR §164.526.
- C. **Accounting of disclosures of PHI and electronic health record.** Assist County to fulfill its obligations to provide accounting of disclosures of PHI under 45 CFR §164.528 and, where applicable, electronic health records under 42 USC §17935(c) if Contractor uses or maintains electronic health records. Contractor shall:
 - (1) Document such disclosures of PHI and/or electronic health records, and information related to such disclosures, as would be required for County to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record in accordance with 45 CFR §164.528.
 - (2) Within fifteen (15) days of receiving a written request from County, provide to County or any individual as directed by County information collected in accordance with this section to permit County to respond to a request by an individual for an accounting of disclosures of PHI and/or electronic health record.
 - (3) Make available for County information required by this Section 6.C for six (6) years preceding the individual's request for accounting of disclosures of PHI, and for three (3) years preceding the individual's request for accounting of disclosures of electronic health record.

7. Security of ePHI. In the event County discloses ePHI to Contractor or Contractor needs to create, receive, maintain, transmit or have access to County ePHI, in accordance with 42 USC §17931 and 45 CFR §164.314(a)(2)(i), and §164.306, Contractor shall:

- A. Comply with the applicable requirements of the Security Rule, and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that Contractor creates, receives, maintains, or transmits on behalf of County in accordance with 45 CFR §164.308, §164.310, and §164.312;

- B. Comply with each of the requirements of 45 CFR §164.316 relating to the implementation of policies, procedures and documentation requirements with respect to ePHI;
 - C. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
 - D. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule;
 - E. Ensure compliance with the Security Rule by Contractor's workforce;
 - F. In accordance with 45 CFR §164.308(b)(2), require that any subcontractors that create, receive, maintain, transmit, or access ePHI on behalf of Contractor agree through contract to the same restrictions and requirements contained in this Addendum and comply with the applicable requirements of the Security Rule;
 - G. Report to County any security incident of which Contractor becomes aware, including breaches of unsecured PHI as required by 45 CFR §164.410; and,
 - H. Comply with any additional security requirements that are applicable to covered entities in Title 42 (Public Health and Welfare) of the United States Code, as may be amended from time to time, including but not limited to HITECH.
8. **Breach of Unsecured PHI.** In the case of breach of unsecured PHI, Contractor shall comply with the applicable provisions of 42 USC §17932 and 45 CFR Part 164, Subpart D, including but not limited to 45 CFR §164.410.
- A. **Discovery and notification.** Following the discovery of a breach of unsecured PHI, Contractor shall notify County in writing of such breach without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except as provided in 45 CFR §164.412.
 - (1) **Breaches treated as discovered.** A breach is treated as discovered by Contractor as of the first day on which such breach is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor, which includes any person, other than the person committing the breach, who is an employee, officer, or other agent of Contractor (determined in accordance with the federal common law of agency).
 - (2) **Content of notification.** The written notification to County relating to breach of unsecured PHI shall include, to the extent possible, the following information if known (or can be reasonably obtained) by Contractor:
 - (a) The identification of each individual whose unsecured PHI has been, or is reasonably believed by Contractor to have been accessed, acquired, used or disclosed during the breach;
 - (b) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
 - (c) A description of the types of unsecured PHI involved in the breach, such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved;

- (d) Any steps individuals should take to protect themselves from potential harm resulting from the breach;
 - (e) A brief description of what Contractor is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,
 - (f) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.
- B. **Cooperation.** With respect to any breach of unsecured PHI reported by Contractor, Contractor shall cooperate with County and shall provide County with any information requested by County to enable County to fulfill in a timely manner its own reporting and notification obligations, including but not limited to providing notice to individuals, prominent media outlets and the Secretary in accordance with 42 USC §17932 and 45 CFR §164.404, §164.406 and §164.408.
- C. **Breach log.** To the extent breach of unsecured PHI involves less than 500 individuals, Contractor shall maintain a log or other documentation of such breaches and provide such log or other documentation on an annual basis to County not later than fifteen (15) days after the end of each calendar year for submission to the Secretary.
- D. **Delay of notification authorized by law enforcement.** If Contractor delays notification of breach of unsecured PHI pursuant to a law enforcement official's statement that required notification, notice or posting would impede a criminal investigation or cause damage to national security, Contractor shall maintain documentation sufficient to demonstrate its compliance with the requirements of 45 CFR §164.412.
- E. **Payment of costs.** With respect to any breach of unsecured PHI caused solely by the Contractor's failure to comply with one or more of its obligations under this Addendum and/or the provisions of HITECH, HIPAA, the Privacy Rule or the Security Rule, Contractor agrees to pay any and all costs associated with providing all legally required notifications to individuals, media outlets, and the Secretary. This provision shall not be construed to limit or diminish Contractor's obligations to indemnify, defend and hold harmless County under Section 9 of this Addendum.
- F. **Documentation.** Pursuant to 45 CFR §164.414(b), in the event Contractor's use or disclosure of PHI and/or ePHI violates the Privacy Rule, Contractor shall maintain documentation sufficient to demonstrate that all notifications were made by Contractor as required by 45 CFR Part 164, Subpart D, or that such use or disclosure did not constitute a breach, including Contractor's completed risk assessment and investigation documentation.
- G. **Additional State Reporting Requirements.** The parties agree that this Section 8.G applies only if and/or when County, in its capacity as a licensed clinic, health facility, home health agency, or hospice, is required to report unlawful or unauthorized access, use, or disclosure of medical information under the more stringent requirements of California Health & Safety Code §1280.15. For purposes of this Section 8.G, "unauthorized" has the meaning given such term in California Health & Safety Code §1280.15(j)(2).
- (1) Contractor agrees to assist County to fulfill its reporting obligations to affected patients and to the California Department of Public Health ("CDPH") in a timely manner under the California Health & Safety Code §1280.15.

- (2) Contractor agrees to report to County any unlawful or unauthorized access, use, or disclosure of patient's medical information without unreasonable delay and no later than two (2) business days after Contractor detects such incident. Contractor further agrees such report shall be made in writing, and shall include substantially the same types of information listed above in Section 8.A.2 (Content of Notification) as applicable to the unlawful or unauthorized access, use, or disclosure as defined above in this section, understanding and acknowledging that the term "breach" as used in Section 8.A.2 does not apply to California Health & Safety Code §1280.15.

9. Hold Harmless/Indemnification.

- A. Contractor agrees to indemnify and hold harmless County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives from any liability whatsoever, based or asserted upon any services of Contractor, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this Addendum, including but not limited to property damage, bodily injury, death, or any other element of any kind or nature whatsoever arising from the performance of Contractor, its officers, agents, employees, subcontractors, agents or representatives from this Addendum. Contractor shall defend, at its sole expense, all costs and fees, including but not limited to attorney fees, cost of investigation, defense and settlements or awards, of County, all Agencies, Districts, Special Districts and Departments of County, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents or representatives in any claim or action based upon such alleged acts or omissions.
- B. With respect to any action or claim subject to indemnification herein by Contractor, Contractor shall, at their sole cost, have the right to use counsel of their choice, subject to the approval of County, which shall not be unreasonably withheld, and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of County; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes Contractor's indemnification to County as set forth herein. Contractor's obligation to defend, indemnify and hold harmless County shall be subject to County having given Contractor written notice within a reasonable period of time of the claim or of the commencement of the related action, as the case may be, and information and reasonable assistance, at Contractor's expense, for the defense or settlement thereof. Contractor's obligation hereunder shall be satisfied when Contractor has provided to County the appropriate form of dismissal relieving County from any liability for the action or claim involved.
- C. The specified insurance limits required in the Underlying Agreement of this Addendum shall in no way limit or circumscribe Contractor's obligations to indemnify and hold harmless County herein from third party claims arising from issues of this Addendum.
- D. In the event there is conflict between this clause and California Civil Code §2782, this clause shall be interpreted to comply with Civil Code §2782. Such interpretation shall not relieve the Contractor from indemnifying County to the fullest extent allowed by law.
- E. In the event there is a conflict between this indemnification clause and an indemnification clause contained in the Underlying Agreement of this Addendum, this indemnification shall only apply to the subject issues included within this Addendum.

10. Term. This Addendum shall commence upon the Effective Date and shall terminate when all PHI and/or ePHI provided by County to Contractor, or created or received by Contractor on behalf of County, is destroyed or returned to County, or, if it is infeasible to return or destroy PHI and/ePHI, protections are extended to such information, in accordance with section 11.B of this Addendum.

11. Termination.

A. **Termination for Breach of Contract.** A breach of any provision of this Addendum by either party shall constitute a material breach of the Underlying Agreement and will provide grounds for terminating this Addendum and the Underlying Agreement with or without an opportunity to cure the breach, notwithstanding any provision in the Underlying Agreement to the contrary. Either party, upon written notice to the other party describing the breach, may take any of the following actions:

- (1) Terminate the Underlying Agreement and this Addendum, effective immediately, if the other party breaches a material provision of this Addendum.
- (2) Provide the other party with an opportunity to cure the alleged material breach and in the event the other party fails to cure the breach to the satisfaction of the non-breaching party in a timely manner, the non-breaching party has the right to immediately terminate the Underlying Agreement and this Addendum.
- (3) If termination of the Underlying Agreement is not feasible, the breaching party, upon the request of the non-breaching party, shall implement, at its own expense, a plan to cure the breach and report regularly on its compliance with such plan to the non-breaching party.

B. **Effect of Termination.**

- (1) Upon termination of this Addendum, for any reason, Contractor shall return or, if agreed to in writing by County, destroy all PHI and/or ePHI received from County, or created or received by the Contractor on behalf of County, and, in the event of destruction, Contractor shall certify such destruction, in writing, to County. This provision shall apply to all PHI and/or ePHI which are in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of PHI and/or ePHI, except as provided below in paragraph (2) of this section.
- (2) In the event that Contractor determines that returning or destroying the PHI and/or ePHI is not feasible, Contractor shall provide written notification to County of the conditions that make such return or destruction not feasible. Upon determination by Contractor that return or destruction of PHI and/or ePHI is not feasible, Contractor shall extend the protections of this Addendum to such PHI and/or ePHI and limit further uses and disclosures of such PHI and/or ePHI to those purposes which make the return or destruction not feasible, for so long as Contractor maintains such PHI and/or ePHI.

12. General Provisions.

A. **Retention Period.** Whenever Contractor is required to document or maintain documentation pursuant to the terms of this Addendum, Contractor shall retain such documentation for 6 years from the date of its creation or as otherwise prescribed by law, whichever is later.

- B. **Amendment.** The parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for County to comply with HITECH, the Privacy Rule, Security Rule, and HIPAA generally.
- C. **Survival.** The obligations of Contractor under Sections 3, 5, 6, 7, 8, 9, 11.B and 12.A of this Addendum shall survive the termination or expiration of this Addendum.
- D. **Regulatory and Statutory References.** A reference in this Addendum to a section in HITECH, HIPAA, the Privacy Rule and/or Security Rule means the section(s) as in effect or as amended.
- E. **Conflicts.** The provisions of this Addendum shall prevail over any provisions in the Underlying Agreement that conflict or appear inconsistent with any provision in this Addendum.
- F. **Interpretation of Addendum.**
 - (1) This Addendum shall be construed to be part of the Underlying Agreement as one document. The purpose is to supplement the Underlying Agreement to include the requirements of the Privacy Rule, Security Rule, HIPAA and HITECH.
 - (2) Any ambiguity between this Addendum and the Underlying Agreement shall be resolved to permit County to comply with the Privacy Rule, Security Rule, HIPAA and HITECH generally.
- G. **Notices to County.** All notifications required to be given by Contractor to County pursuant to the terms of this Addendum shall be made in writing and delivered to the County both by fax and to both of the addresses listed below by either registered or certified mail return receipt requested or guaranteed overnight mail with tracing capability, or at such other address as County may hereafter designate. All notices to County provided by Contractor pursuant to this Section shall be deemed given or made when received by County.

County HIPAA Privacy Officer: HIPAA Privacy Manager

County HIPAA Privacy Officer Address: P.O. Box 1569
Riverside, CA 92502

County HIPAA Privacy Officer Fax Number: (951) 955-HIPAA or (951) 955-4472

————— **TO BE COMPLETED BY COUNTY PERSONNEL ONLY** —————

County Departmental Officer: _____

County Departmental Officer Title: _____

County Department Address: _____

County Department Fax Number: _____

ATTACHMENT IV
PII Privacy and Security Standards

I. PHYSICAL SECURITY

The Contractor shall ensure PII is used and stored in an area that is physically safe from access by unauthorized persons at all times. The Contractor agrees to safeguard PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

- A. Secure all areas of the Contractor facilities where staff assist in the administration of their program and use, disclose, or store PII.
- B. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:
 1. Properly coded key cards
 2. Authorized door keys
 3. Official identification
- C. Issue identification badges to Contractor staff.
- D. Require Contractor staff to wear these badges where PII is used, disclosed, or stored.
- E. Ensure each physical location, where PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.
- F. Ensure there are security guards or a monitored alarm system at all times at the Contractor facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed, or stored. Video surveillance systems are recommended.
- G. Ensure data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only authorized staff. Visitors to the data center area must be escorted at all times by authorized staff.
- H. Store paper records with PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use meaning that there are County and non-County functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within multi-use facilities.
- I. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing PII.

II. TECHNICAL SECURITY CONTROLS

- A. Workstation/Laptop Encryption. All workstations and laptops, which use, store and/or process PII, must be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.

- B. Server Security. Servers containing unencrypted PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
- C. Minimum Necessary. Only the minimum necessary amount of PII required to perform required business functions may be accessed, copied, downloaded, or exported.
- D. Mobile Device and Removable Media. All electronic files, which contain PII data, must be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.
- E. Antivirus Software. All workstations, laptops and other systems, which process and/or store PII, must install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily.
- F. Patch Management.
1. All workstations, laptops and other systems, which process and/or store PII, must have critical security patches applied, with system reboot if necessary.
 2. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
 3. At a maximum, all applicable patches deemed as critical must be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.
 4. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.
- G. User IDs and Password Controls.
1. All users must be issued a unique user name for accessing PII.
 2. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty- four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.
 3. Passwords are not to be shared.
 4. Passwords must be at least eight (8) characters.
 5. Passwords must be a non-dictionary word.
 6. Passwords must not be stored in readable format on the computer or server.
 7. Passwords must be changed every ninety (90) days or less. It is recommended that passwords be required to be changed every sixty (60) days or less.
 8. Passwords must be changed if revealed or compromised.
 9. Passwords must be 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. Lower case letters (a-z)
 - c. Arabic numerals (0-9)
 - d. Special characters (!,@,#, etc.)
- H. Data Destruction. When no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the PII cannot be retrieved.

- I. System Timeout. The systems providing access to PII must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.
- J. Warning Banners. The systems providing access to PII must display a warning banner stating, at a minimum:
 - 1. Data is confidential;
 - 2. Systems are logged;
 - 3. System use is for business purposes only, by authorized users; and
 - 4. Users shall log off the system immediately if they do not agree with these requirements.
- K. System Logging.
 - 1. The systems which provide access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII, or alters PII.
 - 2. The audit trail shall:
 - a. Be date and time stamped;
 - b. Log both successful and failed accesses;
 - c. Be read-access only; and
 - d. Be restricted to authorized users.
 - 3. If PII is stored in a database, database logging functionality shall be enabled.
 - 4. Audit trail data shall be archived for at least three (3) years from the occurrence.
- L. Access Controls. The system providing access to PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.
- M. Transmission Encryption.
 - 1. All data transmissions of PII outside of a secure internal network must be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256 bit encryption be used.
 - 2. Encryption can be end to end at the network level, or the data files containing PII can be encrypted.
 - 3. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.
- N. Intrusion Prevention. All systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, must be protected by an intrusion detection and prevention solution.

III. AUDIT CONTROLS

- A. System Security Review.
 - 1. The Contractor must ensure audit control mechanisms are in place.
 - 2. All systems processing and/or storing PII must have at least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection.
 - 3. Reviews should include vulnerability scanning tools.

- B. Log Reviews. All systems processing and/or storing PII must have a process or automated procedure in place to review system logs for unauthorized access.
- C. Change Control. All systems processing and/or storing PII must have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.

IV. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

- A. Emergency Mode Operation Plan. The Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.
- B. Data Centers. Data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, must include environmental protection such as cooling, power, and fire prevention, detection, and suppression.
- C. Data Backup and Recovery Plan.
 - 1. The Contractor shall have established documented procedures to backup PII to maintain retrievable exact copies of PII.
 - 2. The documented backup procedures shall contain a schedule which includes incremental and full backups.
 - 3. The procedures shall include storing backups offsite.
 - 4. The procedures shall ensure an inventory of backup media.
 - 5. The Contractor shall have established documented procedures to recover PII data.
 - 6. The documented recovery procedures shall include an estimate of the amount of time needed to restore the PII data.

V. PAPER DOCUMENT CONTROLS

- A. Supervision of Data. The PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information.
- B. Data in Vehicles. The Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which staff can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.
- C. Public Modes of Transportation. The PII in paper form shall not be left unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.
- D. Escorting Visitors. Visitors to areas where PII is contained shall be escorted, and PII shall be kept out of sight while visitors are in the area.

- E. Confidential Destruction. PII must be disposed of through confidential means, such as cross cut shredding or pulverizing.
- F. Removal of Data. The PII must not be removed from the premises except for identified routine business purposes or with express written permission of the County.
- G. Faxing.
 - 1. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.
 - 2. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.
 - 3. Fax numbers shall be verified with the intended recipient before sending the fax.
- H. Mailing.
 - 1. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.
 - 2. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the Contractor obtains prior written permission from the County to use another method.

VI. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

During the term of this Agreement, the Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any Breach or Security Incident, and to take the following steps:

The Contractor shall immediately notify the County when it discovers that there may have been a breach in security which has or may have resulted in compromise to confidential data. For purposes of this section, immediately is defined as within two hours of discovery. The County contact for such notification is as follows:

Breaches should be referred to:

DPSS Privacy Officer
Assurance and Review Services
Riverside County Department of Public Social Services
10281 Kidd Street
Riverside, CA 92503
privacyincident@rivco.org