

This Master Services Agreement is entered into as of June 23, 2015 (“Effective Date”), by and between Palantir Technologies Inc., a Delaware corporation, with its principal place of business located at 100 Hamilton Ave., Suite 300, Palo Alto, CA 94301 (“Palantir”) and the County of Santa Clara, with its principal place of business located at 70 W. Hedding Street – East Wing 11<sup>th</sup> Floor, San Jose, CA 95110 (“Customer” or “County” and, collectively with Palantir, the “Parties”).

This Master Services Agreement, including the Terms and Conditions and any Exhibits attached hereto or subsequently entered into by and between the Parties (collectively this “Agreement”), sets forth the terms and conditions pursuant to which Customer will access certain Palantir solutions and contract for certain services from Palantir as set forth in any applicable Statement of Work, the first of which is attached hereto as Exhibit A. Palantir may offer to provide and the Customer may agree to accept additional services by executing additional Statements of Work substantially in the form attached as Exhibit A.

Palantir’s standard support terms and conditions are attached hereto as Exhibit B.

Palantir agrees to comply with all of the terms and conditions set forth in the attached Business Associate Agreement, attached hereto as Exhibit C, which govern and protect the confidentiality, use, and disclosure of confidential data and information provided by the County to Palantir under this agreement.

Palantir confirms that the Cloud Solution to be used in the performance of this agreement conforms to the responses provided in the SCCGov Cloud Service Provider Checklist.

---

**PALANTIR SERVICES TERMS AND CONDITIONS**

1. Certain Definitions. The following capitalized terms will have the meanings indicated below unless otherwise specifically defined in any Exhibits hereto.

1.1 “Client Software” means, if applicable, the software provided by Palantir for installation locally by Customer in order to access the Cloud Solution.

1.2 “Cloud Solution(s)” means Palantir’s service to provide a platform for data analysis, including access to proprietary Palantir software as specified in the Statement of Work, software provided to Customer in connection with this Agreement, and any Updates that are made available in connection with this Agreement (and/or in connection with any future or related Statements of Work, orders, or amendments).

1.3 “Content” means: (a) any data or content that is provided by Customer to Palantir for transmission, storage, integration, import, display, distribution or use in or through use of the Cloud Solutions, including Protected Health Information (PHI) and other private information; and (b) any data, reports or other information generated by the Cloud Solutions to the extent they contain any of the data or content described in the preceding clause (a).

1.4 “Intellectual Property Rights” means patent, copyright, trademark, trade secret and other intellectual or industrial property rights.

1.5 “Software” means the Palantir proprietary software identified on the Statement of Work, any third-party software used to deliver the Cloud Solutions, the Client Software, and any improvements, modifications, derivative works, patches, updates, and upgrades thereto that Palantir develops or provides to Customer hereunder.

1.6 “Term” is defined in Section 9.1.

1.7 “Updates” means Cloud Solution changes that Palantir implements in the applicable generally available Cloud Solution without the payment of additional fees, and associated Client Software updates. Updates do not include new platform services that Palantir makes available for an additional charge.

2. Provision of Cloud Solutions

2.1 Provision of Cloud Solutions. Subject to Customer’s continued and full compliance with all of the terms and conditions of this Agreement, Palantir will provide Customer with access to the Cloud Solution pursuant to the applicable Statement of

Work during the applicable Term associated with such Cloud Solution solely for its internal purposes, and only (i) for use in accordance with the technical specification documentation provided to Customer by Palantir with regard to the Cloud Solutions (“Documentation”) and (ii) for the purposes specified in the applicable Statement of Work.

2.2 Authorized User Accounts. Customer may establish Cloud Solution accounts (“Accounts”) for Customer’s employees or independent contractors with a need to access the Cloud Solutions on behalf of Customer (“Authorized Users”). Customer shall inform each Authorized User of its obligations under, and ensure that each Authorized User at all times abides by the terms of this Agreement. Customer shall immediately notify Palantir in the event that Customer or an Authorized User becomes aware of any violation of the terms of this Agreement. Customer is solely responsible for any use of the Cloud Solutions by Customer’s Authorized Users, and shall be liable for any breach of this Agreement by an Authorized User.

2.3 Account Protection. Customer agrees to provide access to the Client Software and Cloud Solutions only to Authorized Users, and to require such Authorized Users to keep Account login information, including user names and passwords, strictly confidential and not provide such Account login information to any unauthorized parties. Customer is solely responsible for monitoring and controlling access to Account login information in the possession of Customer and its Authorized Users. In the event that Customer or any Authorized User becomes aware that the security of any Account login information has been compromised, Customer shall immediately de-activate such Account or change the Account’s login information. If Palantir discovers or is notified of a breach of security that affects the security of any Content subject to any data breach notification law, Palantir will notify Customer as required by applicable law and under the terms of the Business Associate Agreement (Exhibit C).

2.4 Client Software. Palantir hereby grants to Customer a non-exclusive, nontransferable, limited license to use the Client Software during the Term for the sole purposes of using and receiving Cloud Solutions. At Palantir’s request, Customer will promptly install Updates to the Client Software provided by Palantir.

2.5 Customer Information, Materials and Content. Customer shall provide Palantir with all information, assistance and materials, including access to Content, as reasonably required for Palantir

to activate and operate the Cloud Solutions for Customer pursuant to this Agreement. Customer authorizes Palantir to use, copy, store, process, retrieve, and display such information and materials solely in connection with the provision of the Cloud Solutions for Customer, in accordance with the terms of the Business Associate Agreement (Exhibit C) and all applicable state and federal laws protecting the confidentiality of the information and Content provided. Palantir will store and process Content only in the regions specified in the Statement of Work and will not move Content from such regions without prior written approval of Customer. Palantir is not permitted to disclose Content without Customer’s consent unless (and only to the extent) required to do so pursuant to applicable law.

2.6 Updates. Palantir will have the right to update the Cloud Solutions from time to time, *provided* that Palantir will not materially diminish the functionality or performance of the Cloud Solutions unless such changes are made: (i) to address digital rights management or security issues, (ii) in response to claims, litigation, or loss of license rights related to third-party Intellectual Property Rights, or (iii) to comply with applicable law or regulation or requests or orders of judicial, governmental or regulatory entities.

2.7 Technical Contact. In each Statement of Work, Customer may designate one technical contact as the responsible party for communication with Palantir during provision of the Cloud Solutions under that Statement of Work. Customer may change such contact upon written notice to Palantir.

2.8 Infrastructure. Palantir may host the Cloud Solutions using its own infrastructure or it may engage a third party to host the Cloud Solutions on its behalf (such third-party hosting service a “Third-Party Service”) but only if mutually agreed to in writing by the Parties. The host for the Cloud Solutions shall be specified in each Statement of Work. Customer acknowledges that if a Third Party is utilized to host the Cloud Solution, Palantir is not responsible for the Third Party Services (including without limitation uptime guarantees, outages, or failures) so long as Palantir has used commercially reasonable efforts to obtain appropriate contractual commitments from that Third Party and to enforce those commitments. If Palantir receives a third-party subpoena or request or order of judicial, governmental or regulatory entities regarding Customer’s Account or Content, Palantir will provide Customer with timely notice sufficient to allow Customer to object or seek a protective order, except where providing notice is prohibited by the

legal process itself, by court order, or by applicable law. If Palantir is obligated to respond to a third-party subpoena or other request or order of judicial, governmental or regulatory entities, Palantir will reasonably cooperate with Customer's efforts to seek an appropriate protective order, confidential treatment, or other remedy. Palantir confirms that the Cloud Solution conforms, and covenants that it will continue throughout the Term to conform, to the responses provided in the SCCGov Cloud Service Provider Checklist.

### 3. Proprietary Rights.

3.1 Ownership. Customer acknowledges and agrees that, as between the Parties, Palantir retains all rights, title, and interest in and to the Cloud Solutions, Client Software, Software, Documentation, Updates and any other related documentation or materials provided by Palantir (including without limitation all Intellectual Property Rights embodied in any of the foregoing). Customer shall and hereby does irrevocably transfer and assign to Palantir all right, title, and interest it may have in the foregoing (if any) to Palantir and Palantir hereby accepts such transfer. Except as provided in Section 3.3, no ownership rights are being conveyed to Customer under this Agreement. Except for the express rights granted herein, Palantir does not grant any other licenses or access, whether express or implied, to any Palantir software, services, technology or Intellectual Property Rights. Customer will maintain and not remove, obscure, or alter any copyright notice, trademarks, logos and trade names and any other notices or product identifications that appear on or in any Cloud Solutions, Client Software, Software, Updates or Documentation and any associated media.

3.2 Restrictions. Customer will not (and will not allow any third party to): (i) gain or attempt to gain unauthorized access to the Cloud Solutions, Software or infrastructure, or any element thereof, or circumvent or otherwise interfere with any authentication or security measures of the Cloud Solutions; (ii) interfere with or disrupt the integrity or performance of the Cloud Solutions; (iii) transmit material containing software viruses or other harmful or deleterious computer code, files, scripts, agents, or program through the Cloud Solutions or Software, (iv) decompile, disassemble, reverse engineer or attempt to discover any source code or underlying ideas or algorithms of any Software or the Cloud Solutions (except to the extent that applicable law expressly prohibits such a reverse engineering restriction); (v) provide, lease, lend, use for timesharing or service bureau purposes or otherwise use or allow others to use the Cloud Solutions or

Software for the benefit of any third party; (vi) list or otherwise display or copy any code of any Software; (vii) copy any Software or Cloud Solutions (or component thereof), develop any improvement, modification or derivative work thereof, or include any portion thereof in any other service, equipment or item; (viii) allow the transfer, transmission (including without limitation making available on-line, electronically transmitting, or otherwise communicating, to the public), export, or re-export of any Cloud Solutions, Software or Documentation (or any portion thereof) or any Palantir technical data; (ix) perform benchmark tests on the Cloud Solutions; or (x) use, evaluate or view the Software, Cloud Solutions or Documentation for the purpose of designing, modifying or otherwise creating any environment, program or infrastructure or any portion thereof, which performs functions similar to the functions performed by the Software or Cloud Solutions; *provided, however,* that subject to the other terms and conditions of this Agreement, Customer shall be permitted to develop software that interfaces with Palantir's public APIs, *provided further* that Customer shall not attempt to, or encourage any third party to, sell, rent, lease, license, sublicense, distribute, transfer, or syndicate such software, without prior written approval from Palantir. Notwithstanding the foregoing, or any statement to the contrary herein, portions of the Software or Cloud Solution may be provided or made available with notices and open source or similar licenses from such communities and third parties that govern the use of those portions, and Customer hereby agrees to be bound by and fully comply with all such licenses, and any licenses or access granted hereunder shall not alter any duties or obligations Customer may have under such open source or other licenses; however, the disclaimer of warranty and limitation of liability provisions in this Agreement will apply to all such Software.

3.3 Content. As between the Parties, Customer retains all rights, title, and interest in and to the Content. Palantir shall and hereby does irrevocably transfer and assign to Customer all right, title, and interest it may have in the Content (if any) to Customer and Customer hereby accepts such transfer.

3.4 Usage Data. Palantir may collect analytics, statistics or other data related to the Content and Customer's use of the Cloud Solutions (i) in order to provide the Cloud Solutions to Customer; (ii) for statistical use regarding the Cloud Solutions (provided that such data is not personally identifiable); or (iii) to monitor, analyze, maintain and improve the Cloud Solutions (provided that such data is not personally identifiable).

4. Confidentiality.

4.1 Business Information Exchanged Between the Parties. Pursuant to this Agreement, either Party (the "Disclosing Party") may provide Confidential Information to the other Party (the "Recipient"). Recipient shall keep strictly confidential all Confidential Information (as defined below) of Disclosing Party, and shall not use such Confidential Information except to exercise its rights and perform its obligations herein, and shall not disclose or permit the unauthorized transfer of such Confidential Information to any third party other than disclosure on a need-to-know basis to Recipient's own advisors, attorneys, and/or accountants who are each subject to obligations of confidentiality at least as restrictive as those stated herein. Without limiting the foregoing, Recipient shall use at least the same degree of care as it uses to prevent the disclosure or unauthorized transfer of its own confidential information of like importance, but in no event less than reasonable care. Recipient shall promptly notify Disclosing Party of any actual or suspected misuse or unauthorized disclosure of Disclosing Party's Confidential Information. "Confidential Information" means non-public information that is confidential or proprietary to the Disclosing Party or third parties to which the Disclosing Party owes any duty of confidentiality, and may include, but is not limited to, documents, materials and information regarding or relating to the Disclosing Party's business, programs, assets, personnel, financial condition, results of operations, inventions, discoveries, methods, operations, ideas, concepts, plans, designs, products, processes, know-how, trade secrets, intended uses, technology, software, and/or prospects. Without limiting the scope of the foregoing, "Confidential Information" shall also include (i) Software, Cloud Solutions and Client Software, (including any information or data relating thereto), (ii) Documentation (including any information or data relating thereto), (iii) Customer's Content; and (iv) any other business, technical or engineering information or data (including third-party information) disclosed or made available to Recipient by or on behalf of Disclosing Party which by the nature of the information disclosed or the manner of its disclosure would be understood by a reasonable person to be confidential and/or proprietary, in each case in any form (including without limitation written, electronic, or oral) and whether furnished before, on, or after the Effective Date; *provided, however,* that Confidential Information shall not include any information that (a) is or becomes part of the public domain through no act or omission of Recipient or any of Recipient's employees, agents, advisors, attorneys, accountants, or other representatives, (b) is known to Recipient at

the earlier of the Effective Date or the time of disclosure by Disclosing Party (as evidenced by written records) without an obligation to keep it confidential, (c) was rightfully disclosed to Recipient prior to the Effective Date from another source without any breach of confidentiality by the third-party discloser and without restriction on disclosure or use, or (d) Recipient can document by written evidence that such information was independently developed by Recipient without the use of or any reference or access to Confidential Information, by persons who did not have access to any Confidential Information. Recipient is responsible and shall be liable for any breaches of this Section and any disclosure or misuse of any Confidential Information by its employees or agents (or any other person or entity to which Recipient is permitted to disclose Confidential Information pursuant to this Section). Upon the request of the Disclosing Party, Recipient will return or destroy all Confidential Information of the Disclosing Party that is in its possession. Recipient's obligations with respect to Disclosing Party's Confidential Information shall survive termination of this Agreement for a period of five (5) years; *provided,* that Recipient's obligations hereunder shall survive and continue in perpetuity after termination with respect to any Confidential Information that is a trade secret under applicable law.

4.2 Confidentiality and Protection of Content Provided by County to Palantir. In receiving, maintaining, using, and disposing of Content, Palantir will comply with all applicable state and federal laws regarding the privacy of both the PHI and other private information, including but not limited to:

- (i) The Health Insurance Portability and Accountability Act (HIPAA);
- (ii) The Health Information Technology for Economic and Clinical Health Act (HITECH Act);
- (iii) California Welfare and Institutions Code section 5328;
- (iv) Federal and state constitutional and statutory provisions protecting the privacy of non-health-related private information in the possession of the County, including but not limited to criminal-justice and public benefit-related information.

Further, all Content must be maintained and protected by Palantir in accordance with all of the terms and conditions set forth in the attached Business Associate Agreement (Exhibit C).

5. All Licenses and Services Provided on a Pro Bono Basis. Palantir agrees that the licenses granted and services performed by Palantir under

this agreement are being provided to the County free of charge. Absent mutual agreement of the Parties, under no circumstances will the County be required to provide Palantir with any compensation for the licenses, services, and other deliverables provided under this agreement.

6. Support Services. Palantir shall provide Customer with support and Updates in accordance with and subject to Palantir's standard support terms and conditions ("Support Services") and all Statements of Work (Exhibit(s) A) for the applicable Term. Palantir shall be permitted to access the Customer's instance on-site at the Customer's Premises, via the Cloud Solution, or remotely via a virtual private network or other secure channel solely to provide the services specified hereunder.

7. Training. Palantir agrees to provide its standard training services for the number of Customer personnel specified in the Statement of Work ("Training"), if any.

8. Professional Services. Palantir may provide additional consulting, integration, or other professional services (collectively, "Professional Services") requested by Customer with respect to Customer's use of the Cloud Solutions as may be mutually agreed by the Parties in a Statement of Work. The performance of any Professional Services by Palantir shall not affect the ownership of the Client Software, Cloud Solutions, Documentation and other related documentation or materials provided by Palantir in connection with this Agreement.

9. Term and Termination. This Agreement shall begin on the Effective Date and continue for a period of twelve (12) months from the date of expiration of the last to expire Statement of Work, unless otherwise terminated as provided herein.

9.1 Term. The term of each Statement of Work shall continue for the number of months/years set forth in the Statement of Work unless otherwise terminated as provided herein (each such period a "Term"). During the term of this Agreement, either Party may terminate this Agreement for its convenience with 30 days' prior written notice.

9.2 Extension. The Parties may agree to extend a Term or add additional Terms through the execution of additional Statements of Work. Any future Statements of Work shall be governed by the terms and conditions set forth in this Agreement.

9.3 Termination. Without limiting either Party's other rights of termination set forth in this Agreement, either Party may terminate this Agreement, including the Terms of all then-current Statements of Work, immediately upon written

notice to the other Party in the event of any material breach (as reasonably determined by the non-breaching Party) of any term, condition or provision of this Agreement and failure to remedy the breach (and provide reasonable written notice of such remedy) within thirty (30) days following written notice of such breach.

9.4 Effect of Termination; Survival. Upon any termination or expiration of this Agreement, unless otherwise set forth in a Statement of Work, all of Customer's rights, access and licenses granted hereunder to the Software and Cloud Solutions shall immediately cease and Customer shall promptly return to Palantir or destroy all Client Software and Documentation, including all portions thereof and all other Confidential Information of Palantir, and so certify its compliance with the foregoing to Palantir in writing within ten (10) days of termination or expiration. Upon any termination or expiration of this Agreement, Palantir will provide Customer access to the Content in a format and media reasonably accessible to Customer for ninety (90) days and will thereafter use reasonable methods to delete or otherwise make all such Content inaccessible. No termination or expiration of this Agreement shall limit or affect either party's rights or obligations that accrued prior to the effective date of termination or expiration. Furthermore, this Section 9.4 (Effect of Termination; Survival) and Sections 3 (Proprietary Rights), 4 (Confidentiality), 5, 9.5 (Post-Termination Transition), 10 (Indemnification), 11.2 (Disclaimer), 13 (Limitations of Liability), 14 (Dispute Resolution), 15 (Miscellaneous), 16 (Government Matters), and 17 (Third Party Data) shall survive any termination or expiration of this Agreement. Termination is not an exclusive remedy and all other remedies will remain available. All non-expired Statements of Work shall automatically terminate upon the termination of this Agreement.

9.5 Post-Termination Transition. Upon written request by Customer, Palantir shall, following termination of this Agreement, provide reasonable transition assistance to Customer for a period of ninety (90) days in order to minimize disruption to Customer's business.

10. Indemnification for Claims of Intellectual Property Right Infringement.

Palantir shall defend Customer against any claim of infringement or violation of any U.S. patent, copyright, or trademark asserted against Customer by a third party based upon Customer's use of the Cloud Solutions in accordance with the terms of this Agreement and indemnify and hold harmless Customer from and against damages, costs, and attorneys' fees, if any, finally awarded pursuant to a

non-appealable order by a court of competent jurisdiction in such claim or settlement entered into by Palantir, *provided* that Palantir shall have received from Customer: (i) notice of such claim within ten (10) days of Customer receiving proper service of such claim (provided that failure to provide notice within the time specified above will excuse Palantir from its obligations under this Section 10 only to the extent such delay actually prejudices Palantir's defense of the claim); (ii) the exclusive right to control and direct the investigation, defense, and settlement (if applicable) of such claim; and (iii) all reasonable necessary cooperation of Customer. If Customer's use of any of the Cloud Solutions is, or in Palantir's opinion is likely to be, enjoined by a court of competent jurisdiction due to the type of infringement specified above, or if required by settlement approved by Palantir in writing, Palantir may, in its sole discretion: (a) substitute for the Cloud Solutions substantially functionally similar services and documentation; (b) procure for Customer the right to continue using the Cloud Solutions; or (c) if Palantir reasonably determines that options (a) and (b) are commercially impracticable, terminate this Agreement and refund to Customer a pro-rated portion of the fees paid hereunder for the terminated Cloud Solutions that reflects the remaining portion of the Term(s) of any Statements of Work in effect at the time of termination. The foregoing obligations of Palantir shall not apply: (1) if the Cloud Solutions are modified by any party other than Palantir, but only to the extent the alleged infringement would not have occurred but for such modification; (2) if the Cloud Solutions are modified by Palantir at the request of Customer, but only to the extent the alleged infringement would not have occurred but for such modification; (3) if the Cloud Solutions are combined with other non-Palantir products or processes not authorized by Palantir, but only to the extent the alleged infringement would not have occurred but for such combination; (4) to any unauthorized use of the Cloud Solutions, any use that is not consistent with the Documentation, or use during any period of suspension; (5) to any superseded release of the Client Software if the infringement would have been avoided by the use of a current release of the Client Software that Palantir has provided or made available to Customer prior to the date of the alleged infringement; (6) to any Content; or (7) to any third-party products, software or services contained within or used to deliver the Cloud Solutions (including any open source software). THIS SECTION SETS FORTH PALANTIR'S SOLE LIABILITY AND OBLIGATION AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY THIRD-PARTY CLAIM OF

## INTELLECTUAL PROPERTY RIGHTS INFRINGEMENT.

11. **Indemnification for All Other Claims.** Palantir shall indemnify, defend, and hold harmless the County, its officers, agents and employees from any claim, liability, loss, injury or damage arising out of this Agreement, but only in proportion to and to the extent such claim, liability, loss, injury or damage is caused by or result from the negligent or intentional acts or omissions of Palantir, its officers, employees, or agents. County shall indemnify, defend, and hold harmless Palantir, its officers, agents and employees from any claim, liability, loss, injury or damage arising out of this Agreement, but only in proportion to and to the extent such claim, liability, loss, injury or damage is caused by or result from the negligent or intentional acts or omissions of County, its officers, employees, or agents.

### 12. Palantir Limited Warranty and Disclaimer.

12.1 **Limited Warranty.** Subject to the terms and conditions set forth in this Section 12 Palantir warrants that for a period of thirty (30) days after activation the Cloud Solutions will substantially conform to Palantir's then-current Documentation for such Cloud Solutions. This warranty covers only problems reported to Palantir in writing (including full documentation of the failure). In the event of a material failure of the Cloud Solutions to perform substantially in accordance with the Documentation during the warranty period ("Defect"), Palantir shall use reasonable efforts to correct the Defect or provide a suitable work around as soon as reasonably practical after receipt of Customer's written notice as specified above. A Defect shall not include any defect or failure attributable to improper use, misuse or abuse of the Cloud Solutions. If Palantir has not remedied the Defect within thirty (30) days of its receipt of Customer's written notice, Customer may give Palantir written notice of termination of this Agreement, which termination will be effective thirty (30) days after Palantir's receipt of the notice, unless Palantir is able to remedy the Defect prior to the effective date of termination. In the event of the termination of this Agreement pursuant to Customer's exercise of its right under this Section, Customer shall be entitled to receive from Palantir, as its sole and exclusive remedy, a refund of a pro-rated portion of the fees paid hereunder, if any, for the terminated Cloud Solutions that reflects the remaining portion of the Term(s) of any Statements of Work in effect at the time of termination but such termination shall otherwise be subject to Section 11.2. Further, Palantir warrants that Client Software and Cloud Services do not knowingly contain, and will not knowingly expose Customer's software,

systems or Content to, any viruses, back doors, or other malicious code.

12.2 Disclaimer. AS APPLICABLE, NO AMOUNTS PAID HEREUNDER ARE REFUNDABLE OR OFFSETTABLE EXCEPT AS SET FORTH IN SECTION 12.1. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 12.1 AND 13.2, AND WITHOUT LIMITING PALANTIR'S OBLIGATIONS UNDER SECTION 6 AND/OR EXHIBIT B, THE SERVICES ARE PROVIDED "AS-IS" WITHOUT ANY OTHER WARRANTIES OF ANY KIND AND PALANTIR AND ITS SUPPLIERS AND SERVICE PROVIDERS HEREBY DISCLAIM ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, ORAL OR WRITTEN, RELATING TO THE PRODUCTS AND ANY SERVICES PROVIDED HEREUNDER OR SUBJECT MATTER OF THIS AGREEMENT OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, TITLE OR FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITING THE FOREGOING LIMITATION, PALANTIR DOES NOT WARRANT THAT THE SERVICES, SOFTWARE, DOCUMENTATION OR TRAINING WILL MEET CUSTOMER REQUIREMENTS OR THAT OPERATION OF CLOUD SOLUTIONS WILL BE UNINTERRUPTED OR ERROR FREE. CUSTOMER ACKNOWLEDGES THAT PALANTIR DOES NOT CONTROL THE TRANSFER OF DATA, INFORMATION OR CONTENT OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET OR THIRD-PARTY SERVICE, AND THAT THE CLOUD SOLUTIONS MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH COMMUNICATIONS FACILITIES. PALANTIR IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS.

### 13. Customer Representations and Warranties.

13.1 General. Customer represents, warrants, and covenants to Palantir that, to the knowledge of Customer, neither this Agreement (or any term hereof) nor the performance of or exercise of rights under this Agreement is restricted by, contrary to, in conflict with, ineffective under, requires registration or approval or tax withholding under, or affects Customer's proprietary rights (or the duration thereof) under, or will require any termination payment or compulsory licensing under, any law or regulation of any country, group of countries or political or governmental entity located within or

including all or a portion of any geographic area where the Cloud Solutions or any part thereof (whether or not incorporated with or into other software) will be used.

13.2 Use of Cloud Solutions. Customer represents, warrants and covenants to Palantir that it will not use the Cloud Solutions for any unauthorized, improper or illegal purposes, including but not limited to (i) unlawful discrimination, (ii) harassment, (iii) compromising information and data security or confidentiality, (iv) harmful or fraudulent activities, (v) violation of privacy or constitutional rights of individuals or organizations, and/or (vi) violation of contractual agreement or local, state, and/or Federal laws, regulations, or ordinances. Palantir represents, warrants and covenants to Customer that it will not use the Content or Cloud Solutions for any unauthorized, improper or illegal purposes, including but not limited to (i) unlawful discrimination, (ii) harassment, (iii) compromising information and data security or confidentiality, (iv) harmful or fraudulent activities, (v) violation of privacy or constitutional rights of individuals or organizations, and/or (vi) violation of contractual agreement or local, state, and/or Federal laws, regulations, or ordinances.

14. Customer Content. Customer represents, warrants and covenants to Palantir that (i) it will not transmit, store, integrate, import, display, distribute, use or otherwise make available any Content that is, or is obtained in a manner that is, unauthorized, improper or illegal; (ii) no Content infringes upon or violates any other party's Intellectual Property Rights, privacy, publicity or other proprietary rights (so long as Palantir treats such Content in accordance with the requirements of this Agreement); (iii) this Agreement imposes no obligations, by contract or local, state, Federal, international law, regulation or ordinance, with respect to Content, other than those expressly set forth or referenced in this Agreement and any Statement of Work. Customer acknowledges that all Content that Customer transmits, stores, integrates, imports, displays, distributes, uses or otherwise makes available through use of the Cloud Solutions and the conclusions drawn therefrom are done at Customer's own risk and Customer will be solely liable and responsible for any damage or losses to any party resulting therefrom unless such damage or losses result from the failure of the Cloud Solution to perform in accordance with the terms of this agreement, Palantir's then-current documentation, or from the negligence or willful misconduct on the part of Palantir's employees or agents. Palantir has the right to immediately suspend the Cloud Solutions (a) in order to prevent harm to Palantir or its business and to limit any potential liability, (b) if

Customer is in breach of this Agreement, or (c) if required to do so pursuant to applicable law or regulation or requests or orders of judicial, governmental or regulatory entities.

15. Limitations of Liability.

15.1 No Consequential Damages. EXCEPT FOR PALANTIR'S OBLIGATIONS SET FORTH IN SECTIONS 4 AND 10 OF THIS AGREEMENT, AND EXCEPT FOR BODILY INJURY (BUT SOLELY TO THE EXTENT THAT LIMITATION ON LIABILITY THEREFOR IS NOT PERMITTED UNDER APPLICABLE LAW), TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY OR TO ANY THIRD PARTY WITH RESPECT TO ANY PRODUCT, SERVICE OR OTHER SUBJECT MATTER OF THIS AGREEMENT FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, REGARDLESS OF THE LEGAL THEORY USED TO MAKE A CLAIM, AND WHETHER OR NOT BASED UPON THE PARTY'S NEGLIGENCE, BREACH OF WARRANTY, STRICT LIABILITY, IN TORT OR ANY OTHER CAUSE OF ACTION, INCLUDING WITHOUT LIMITATION, LOSS OF USE, LOSS, ALTERATION, CORRUPTION, OR BREACH OF DATA, COST OF REPLACEMENT, DELAYS, LOST PROFITS, OR SAVINGS ARISING OUT OF PERFORMANCE OR BREACH OF THIS AGREEMENT OR THE USE OR INABILITY TO USE THE CLOUD SOLUTIONS, OR FOR ANY MATTER BEYOND THE PARTY'S REASONABLE CONTROL, EVEN IF THE PARTY HAS BEEN ADVISED AS TO THE POSSIBILITY OF SUCH DAMAGES.

15.2 Cap. EXCEPT FOR PALANTIR'S OBLIGATIONS SET FORTH IN SECTIONS 4 AND 10 OF THIS AGREEMENT, AND EXCEPT FOR BODILY INJURY (BUT SOLELY TO THE EXTENT THAT LIMITATION ON LIABILITY THEREFOR IS NOT PERMITTED UNDER APPLICABLE LAW), TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, EACH PARTY AGREES THAT THE MAXIMUM AGGREGATE LIABILITY OF ANY CLAIM OF ANY KIND, WHETHER BASED ON CONTRACT, TORT (INCLUDING BUT NOT LIMITED TO, STRICT LIABILITY, PRODUCT LIABILITY OR NEGLIGENCE) OR ANY OTHER LEGAL OR EQUITABLE THEORY OR RESULTING FROM THIS AGREEMENT OR

ANY PRODUCTS OR SERVICES FURNISHED HEREUNDER SHALL NOT EXCEED THE GREATER OF (A) THE FEES PAID TO PALANTIR BY CUSTOMER HEREUNDER OR (B) \$100,000 AND THAT SUCH REMEDY IS FAIR AND ADEQUATE.

16. Governing Law and Venue. This Agreement shall be deemed to have been made in, and shall be construed pursuant to the laws of the State of California and the United States, without regard to conflicts of law provisions thereof, and without regard to the United Nations Convention on contracts for the International Sale of Goods. The Parties consent to exclusive jurisdiction and venue in the United States Federal Courts located in the Northern District of California or California Superior Court in the County of Santa Clara.

17. Miscellaneous. Neither this Agreement nor the access, obligations, or licenses granted hereunder may be assigned, transferred, subcontracted, or sublicensed by Customer or Palantir; any attempt to do so shall be void. Notwithstanding the foregoing, Palantir may assign this Agreement in whole or in part to an entity acquiring all or substantially all of Palantir's assets. Any notice, report, approval or consent required or permitted hereunder shall be in writing and sent by first class U.S. mail, confirmed facsimile, or major commercial rapid delivery courier service to the address specified in the applicable Statement of Work. If any provision of this Agreement shall be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and be enforceable. Any and all modifications, waivers or amendments must be made by mutual agreement and shall be effective only if made in writing and signed by each Party. No waiver of any breach shall be deemed a waiver of any subsequent breach. Customer's rights under this Agreement are subject to its compliance with all applicable export control laws and regulations. Neither Party will be liable for any failure or delay in its performance under this Agreement due to any cause beyond its reasonable control, including without limitation acts of war, acts of God, earthquake, flood, embargo, riot, sabotage, labor shortage or dispute, governmental act or failure of the Internet, telecommunications or hosting service provider, computer attacks, or malicious acts; *provided* that the delayed Party: (i) gives the other Party prompt notice of such cause, and (ii) uses its commercially reasonable efforts promptly to correct such failure or delay in performance. This Agreement, including any Exhibits hereto and any mutually executed Statements of Work, together



with any confidentiality or non-disclosure agreement entered into by and between the Parties, is the complete and exclusive statement of the mutual understanding of the Parties and supersedes and cancels all previous written and oral agreements and communications relating to the subject matter of this Agreement. In the event of a conflict between this Agreement and any Exhibits, Statements of Work, or other documentation entered into between the Parties, the terms and conditions of the Business Associates Agreement (Exhibit C) will prevail with respect to the handling of Protected Information, and the terms and conditions of this Agreement will prevail with respect to all other provisions. Palantir is in no way affiliated with, or endorsed or sponsored by, The Saul Zaentz Company d.b.a. Tolkien Enterprises or the Estate of J.R.R. Tolkien.

17. Government Matters. The Cloud Solution, Software, Documentation, Support Services, Training and Professional Services are "commercial items" as defined at 48 C.F.R. 2.101, consisting of "commercial computer software, commercial computer software documentation and commercial services". If Customer or end user is a U.S. governmental entity, then Customer acknowledges and agrees that (i) use, duplication, reproduction, release, modification, disclosure, or transfer of the Products and any related documentation of any kind, including, without limitation, technical data and manuals, will be restricted in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes, (ii) the Products were developed fully at private expense and (iii) all other use of the Products except in accordance with the license grant provided above is strictly prohibited.

18. County's Standard Terms.

18.1 Conflicts of Interest.

(a) Palantir shall comply, and require its subcontractors to comply, with all applicable (i) requirements governing avoidance of impermissible client conflicts; and (ii) federal, state and local conflict of interest laws and regulations including, without limitation, California Government Code section 1090 et. seq., the California Political Reform Act (California Government Code section 87100 et. seq.) and the regulations of the Fair Political Practices Commission concerning disclosure and disqualification (2 California Code of Regulations section 18700 et. seq.). Failure to do so constitutes a material breach of this Agreement and is grounds for immediate termination of this Agreement by the County.

(b) In accepting this Agreement, Palantir covenants that it presently has no interest, and will not acquire any interest, direct or indirect, financial or otherwise, which would conflict in any manner or degree with the performance of this Agreement. Palantir further covenants that, in the performance of this Agreement, it will not employ any contractor or person having such an interest. Palantir, including but not limited to Palantir's employees and subcontractors, may be subject to the disclosure and disqualification provisions of the California Political Reform Act of 1974 (the "Act"), that (1) requires such persons to disclose economic interests that may foreseeably be materially affected by the work performed under this Agreement, and (2) prohibits such persons from making or participating in making decisions that will foreseeably financially affect such interests.

(c) If the disclosure provisions of the Political Reform Act are applicable to any individual providing service under this Agreement, Palantir shall, upon execution of this Agreement, provide the County with the names, description of individual duties to be performed, and email addresses of all individuals, including but not limited to Palantir's employees, agents and subcontractors, that could be substantively involved in "making a governmental decision" or "serving in a staff capacity and in that capacity participating in making governmental decisions or performing duties that would be performed by an individual in a designated position," (2 CCR 18701(a)(2)), as part of Palantir's service to the County under this Agreement. Palantir shall immediately notify the County of the names and email addresses of any additional individuals later assigned to provide such service to the County under this Agreement in such a capacity. Palantir shall immediately notify the County of the names of individuals working in such a capacity who, during the course of the Agreement, end their service to the County.

(d) If the disclosure provisions of the Political Reform Act are applicable to any individual providing service under this Agreement, Palantir shall ensure that all such individuals identified pursuant to this section understand that they are subject to the Act and shall conform to all requirements of the Act and other laws and regulations listed in subsection (A) including, as required, filing of Statements of Economic Interests within 30 days of commencing service pursuant to this Agreement, annually by April 1, and within 30 days of their termination of service pursuant to this Agreement.

18.2 Grant Agreements. Palantir will cooperate with County in complying with the provided terms of all federal, state, and philanthropic funding agreements under which the County is a Grantee that apply to the services performed under this Agreement.

18.3 Assignment of Clayton Act, Cartwright Act Claims. Palantir assigns to the County all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. Sec. 15) or under the Cartwright Act (Chapter 2 (commencing with Section 16700) of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of goods, materials, or services by the Palantir for sale to the County pursuant to this Agreement.

18.4 Non-Discrimination. Palantir shall comply with all applicable Federal, State, and local laws and regulations including Santa Clara County's policies concerning nondiscrimination and equal opportunity in contracting. Such laws include but are not limited to the following: Title VII of the Civil Rights Act of 1964 as amended; Americans with Disabilities Act of 1990; The Rehabilitation Act of 1973 (Sections 503 and 504); California Fair Employment and Housing Act (Government Code sections 12900 et seq.); and California Labor Code sections 1101 and 1102. Palantir shall not discriminate against any subcontractor, employee, or applicant for employment because of age, race, color, national origin, ancestry, religion, sex/gender, sexual orientation, mental disability, physical disability, medical condition, political beliefs, organizational affiliations, or marital status in the recruitment, selection for training including apprenticeship, hiring, employment, utilization, promotion, layoff, rates of pay or other forms of compensation. Nor shall Palantir discriminate in provision of services provided under this contract because of age, race, color, national origin, ancestry, religion, sex/gender, sexual orientation, mental disability, physical disability, medical condition, political beliefs, organizational affiliations, or marital status.

18.5 County No-Smoking Policy. Palantir and its employees, agents and subcontractors, shall comply with the County's No-Smoking Policy, as set forth in the Board of Supervisors Policy Manual section 3.47 (as amended from time to time), which prohibits smoking: (1) at the Santa Clara Valley Medical Center Campus and all County-owned and operated health facilities, (2) within 30 feet surrounding County-owned buildings and leased buildings where the County is the sole occupant, and (3) in all County vehicles.

18.6 Food and Beverage Standards. Except in the event of an emergency or medical necessity, the following nutritional standards shall apply to any foods and/or beverages purchased by Palantir with County funds for County-sponsored meetings or events. If food is to be provided, healthier food options shall be offered. "Healthier food options" include (1) fruits, vegetables, whole grains, and low fat and low calorie foods; (2) minimally processed foods without added sugar and with low sodium; (3) foods prepared using healthy cooking techniques; and (4) foods with less than 0.5 grams of trans fat per serving. Whenever possible, Palantir shall (1) offer seasonal and local produce; (2) serve fruit instead of sugary, high calorie desserts; (3) attempt to accommodate special, dietary and cultural needs; and (4) post nutritional information and/or a list of ingredients for items served. If meals are to be provided, a vegetarian option shall be provided, and the Palantir should consider providing a vegan option. If pre-packaged snack foods are provided, the items shall contain: (1) no more than 35% of calories from fat, unless the snack food items consist solely of nuts or seeds; (2) no more than 10% of calories from saturated fat; (3) zero trans fat; (4) no more than 35% of total weight from sugar and caloric sweeteners, except for fruits and vegetables with no added sweeteners or fats; and (5) no more than 360 mg of sodium per serving. If beverages are to be provided, beverages that meet the County's nutritional criteria are (1) water with no caloric sweeteners; (2) unsweetened coffee or tea, provided that sugar and sugar substitutes may be provided as condiments; (3) unsweetened, unflavored, reduced fat (either nonfat or 1% low fat) dairy milk; (4) plant-derived milk (e.g., soy milk, rice milk, and almond milk) with no more than 130 calories per 8 ounce serving; (5) 100% fruit or vegetable juice (limited to a maximum of 8 ounces per container); and (6) other low-calorie beverages (including tea and/or diet soda) that do not exceed 40 calories per 8 ounce serving. Sugar-sweetened beverages shall not be provided.

18.7 Contracting Principles. All entities that contract with the County to provide services where the contract value is \$100,000 or more per budget unit per fiscal year and/or as otherwise directed by the Board, shall be fiscally responsible entities and shall treat their employees fairly. To ensure compliance with these contracting principles, Palantir shall: (1) comply with all applicable federal, state and local rules, regulations and laws; (2) maintain financial records, and make those records available upon request; (3) provide to the County copies of any financial audits that have been completed during the term of the contract; (4) upon the County's request, provide the County reasonable

access, through representatives of Palantir, to facilities, financial and employee records that are related to the purpose of the contract, except where prohibited by federal or state laws, regulations or rules.

18.8 California Public Records Act. All proposals become the property of the County, which is a public agency subject to the disclosure requirements of the California Public Records Act ("CPRA"). If Palantir proprietary information is contained in documents submitted to County, and Palantir claims that such information falls within one or more CPRA exemptions, Palantir must clearly mark such information "CONFIDENTIAL AND PROPRIETARY," and identify the specific lines containing the information. In the event of a request for such information, the County will make best efforts to provide notice to Palantir prior to such disclosure. If Palantir contends that any documents are exempt from the CPRA and wishes to prevent disclosure, it is required to obtain a protective order, injunctive relief or other appropriate remedy from a court of law in Santa Clara County before the County responds to the CPRA request. If Palantir fails to obtain such a remedy before the County responds to the CPRA request, County may disclose the requested information. Palantir further agrees that it shall defend, indemnify and hold County harmless against any claim, action or litigation (including but not limited to all judgments, costs, fees, and attorney's fees) that may result from denial by County of a CPRA request for information arising from any representation, or any action (or inaction), by the Palantir.

18.9 Wage Theft Prevention.

(a) Compliance with Wage and Hour Laws: Palantir, and any subcontractor it employs to complete work under this Agreement, must comply with all applicable federal, state, and local wage and hour laws. Applicable laws may include, but are not limited to, the Federal Fair Labor Standards Act, the California Labor Code, and any local Minimum Wage Ordinance or Living Wage Ordinance.

(b) Final Judgments, Decisions, and Orders: For purposes of this Section, a "final judgment, decision, or order" refers to one for which all appeals have been exhausted. Relevant investigatory government agencies include: the federal Department of Labor, the California Division of Labor Standards Enforcement, a local enforcement agency, or any other government entity tasked with the investigation and enforcement of wage and hour laws.

(c) Prior Judgments against Palantir and/or its Subcontractors: BY SIGNING THIS AGREEMENT, PALANTIR AFFIRMS THAT IT HAS DISCLOSED ANY FINAL JUDGMENTS, DECISIONS, OR ORDERS FROM A COURT OR INVESTIGATORY GOVERNMENT AGENCY FINDING—IN THE FIVE YEARS PRIOR TO EXECUTING THIS AGREEMENT—THAT PALANTIR OR ITS SUBCONTRACTOR(S) HAS VIOLATED ANY APPLICABLE WAGE AND HOUR LAWS. PALANTIR FURTHER AFFIRMS THAT IT OR ITS SUBCONTRACTOR(S) HAS SATISFIED AND COMPLIED WITH—OR HAS REACHED AGREEMENT WITH THE COUNTY REGARDING THE MANNER IN WHICH IT WILL SATISFY—ANY SUCH JUDGMENTS, DECISIONS, OR ORDERS.

(d) Judgments During Term of Contract: If at any time during the term of this Agreement, a court or investigatory government agency issues a final judgment, decision, or order finding that Palantir or any subcontractor it employs to perform work under this Agreement has violated any applicable wage and hour law, or Palantir learns of such a judgment, decision, or order that was not previously disclosed, Palantir must inform the Office of the County Executive-Countywide Contracting, no more than 15 days after the judgment, decision, or order becomes final or of learning of the final judgment, decision or order. Palantir and its subcontractors shall promptly satisfy and comply with any such judgment, decision, or order, and shall provide the Office of the County Executive-Countywide Contracting with documentary evidence of compliance with the final judgment, decision or order within 5 days of satisfying the final judgment, decision, or order. The County reserves the right to require Palantir to enter into an agreement with the County regarding the manner in which any such final judgment, decision or order will be satisfied.

(e) County's Right to Withhold Payment: Where Palantir or any subcontractor it employs to perform work under this Agreement has been found in violation of any applicable wage and hour law by a final judgment, decision, or order of a court or government agency, the County reserves the right to withhold payment to Palantir until such judgment, decision, or order has been satisfied in full.

(f) Material Breach: Failure to comply with any part of this Section constitutes a material breach of this Agreement. Such breach may serve as a basis for termination of this Agreement and/or any other remedies available under this Agreement and/or law.

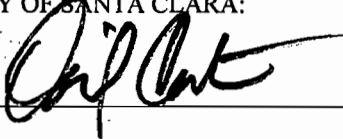
(g) Notice to County Related to Wage Theft Prevention: Notice provided to the Office of the County Executive as required under this Section shall be addressed to: Office of the County Executive—Countywide Contracting; 70 West Hedding Street; East Wing, 11th Floor; San José, CA 95110. The Notice provisions of this Section are separate from any other notice provisions in this Agreement and, accordingly, only notice provided to the above address satisfies the notice requirements in this Section.

IN WITNESS WHEREOF, the Parties have executed this Statement of Work #\_\_ to the Master Services Agreement as of the later date set forth below.

**SIGNATURES**

---

COUNTY OF SANTA CLARA:

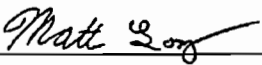
By: 

Name: Dave Cortese

Title: President, Board of Supervisors

Date: JUN 23 2015

PALANTIR TECHNOLOGIES INC.

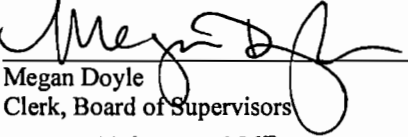
By: 

Name: Matt Long

Title: Legal Counsel

Date: June 18, 2015

ATTEST:

  
Megan Doyle  
Clerk, Board of Supervisors

Date: JUN 23 2015

APPROVED AS TO FORM AND LEGALITY:

  
Greta S. Hansen  
Lead Deputy County Counsel

Date: 6/15/15

## EXHIBIT A

### **Statement of Work**

This Statement of Work is issued pursuant to the Master Services Agreement, including the Terms and Conditions and any Exhibits attached thereto (collectively, the "Agreement"), entered into between the Parties on June 23, 2015, which sets forth the terms and conditions pursuant to which Customer will access certain Palantir solutions and contract for certain services from Palantir and pursuant to which Palantir will provide such services to Customer.

#### **Executive Summary**

The goal of this initiative is to partner with Santa Clara County ("The County") to provide the technical infrastructure for their Pay for Success ("PFS") initiative to combat chronic homelessness in The County. Palantir will provide technology ("The Platform") to help The County identify the subset of chronically homeless individuals who are the most costly users of County services.

Palantir engineers will integrate the data sources identified by The County as critical to triage decisions into the The Platform. We will implement a triage tool to help service providers selected by The County in providing appropriate interventions to the most vulnerable and needy homeless population. Palantir will provide the necessary engineers to facilitate data integration and data presentation, as well as support from Palantir's dedicated Privacy and Civil Liberties Team to help ensure proper handling of sensitive data.

We expect that this Platform can also be extended to address other social sector use cases, should The County decide to use it as such.

This document outlines our initial project plan for Phase 1 of this project, which will focus on:

- Accessing and onboarding key data sources
- Team structure and onboarding of key personnel
- Triage tool development and deployment
- Evaluation support

#### **PROJECT OVERVIEW**

The project will create a tool for triaging candidates for recruitment into the Permanent Supportive Housing (PSH) program. Candidates will be identified by 1) applying UCSF's triage tool in The Platform against data integrated from a set of relevant systems or 2) applying screening tools against candidates referred by select County agencies (see "Santa Clara County Pay for Success Draft Evaluation Plan," hereafter the Evaluation Plan), as well as supporting the ability of County personnel to surface information that facilitates confirmation that prospective candidates are currently chronically homeless.

#### **(I) Project preparation**

Successful rollout of the triage tool within the target timeline relies on up-front preparation across several areas. In particular:

##### **Obtaining permission to access data sources**

Accessing healthcare related data sources and law enforcement data sources will require completion of certain administrative approval processes and support from data owners. Execution of all legal documents required to access these confidential data sources and completion of any necessary administrative approval

processes will need to be completed before Palantir engineers may commence working with these sensitive data sets.

### Obtaining network access data sources

After the necessary permissions for data access have been granted, Palantir engineers will need technical assistance to establish connections to the required data sources and the networks in which these data sources reside. Data source accounts must be created to support read-only backend access or, where appropriate, web service access, and network access must be granted as appropriate. This must also be completed before integration work can commence.

### Establish triage criteria

A first pass of criteria definition will be completed as early as possible in order to enable engineers to target data fields in each data set.

### (2) Data Integration

The systems listed in the table below have been identified as candidates for integration into Palantir's platform to facilitate triage analysis.

Note that integrating any of the data requires completion of all steps listed in the previous section for that specific system.

SYSTEM	DESCRIPTION
<b>Santa Clara Valley Health and Hospital System (HealthLink &amp; Unicare)</b>	Physical and mental health information including: <ul style="list-style-type: none"><li>• County inpatient and emergency room care for homeless residents</li></ul> Mental health and substance abuse treatment information including: <ul style="list-style-type: none"><li>• Utilization information regarding specialty mental health and substance abuse treatment services</li><li>• Involuntary psychiatric evaluation and treatment</li></ul>
<b>Criminal Justice Information Control (CJIC)</b>	Tracks individuals from arrest to adjudication in the County of Santa Clara, including: <ul style="list-style-type: none"><li>• Arrests</li><li>• Bookings</li><li>• Jail sentence information</li><li>• Probation information</li></ul>
<b>ELMR</b>	Custody Health Services <ul style="list-style-type: none"><li>• Medical, mental health, and pharmacy services provided to residents/detainees of the Receiving/Assessment Intake Center, Juvenile Hall, the James Ranch, Main Jail, and the Elmwood complex</li></ul>

<b>Homeless Management Information System (HMIS)</b>	Tracks housing assistance and supportive services utilization of unhoused and very low-income residents of the county.  <i>Will not integrate this database directly.</i> Key information needed is list of approximately 9700 chronically homeless people tracked in HMIS, which can be imported into Palantir without integration. As the County transitions their HMIS service provider, Palantir, UCSF researchers, and County personnel will mutually identify additional data fields that may assist in screening and chronic homeless verification.
--	--

As data is integrated from the systems above, Palantir will work in conjunction with UCSF researchers and relevant County personnel to identify and capture information that may assist in chronic homelessness triage and verification.

To the extent that any of the data systems cannot be accessed through the type of direct database connection that is standard for Palantir integrations, a procedure for regularly and consistently extracting data from those databases for Palantir will be established.

The systems listed above are also likely to contain data on a partially overlapping set of people. However, these systems may lack a unique identifier that can be used to easily match persons across the systems. After data has been integrated, Palantir engineers and County personnel will work together to devise optimal criteria for linking records across data sets given the range of available identifiers. When the agreed upon criteria cannot automatically identify a match across data sets, Palantir will provide tools to enable the County Study Team to manually perform such matching.

### **(3) Triage and reporting**

Palantir will enable the Study Team to identify candidates who meet the defined selection criteria for the Permanent Supportive Housing Program from the set of all persons with available records, consistent with the County Evaluation Plan. Palantir will, at a minimum, enable data exports on candidates to common and most useful formats (e.g., Excel Spreadsheets, CSVs, etc.). If the triage export does not contain sufficient information on each candidate, an alternate export format may be developed that will provide a detailed profile of individual candidates.

Palantir will also conduct user interviews with relevant County personnel and UCSF researchers to identify workflows suitable for specific web application solutions to assist in triage, management, enrollment, and evaluation consistent with the County's Evaluation Plan. Palantir intends to test and deploy a web-based dashboard to enhance situational awareness among key County staff. The tools will enable users to 1) take appropriate action on client alerts from relevant County referral points and 2) manage generated lists of clients, consistent with the Evaluation Plan. Any web-based solution is contingent on reasonable user-testing time with County staff and consistent with the needs outlined in the County Evaluation Plan.

### **(4) Evaluation**

Using Palantir's flexible analytical platform, County personnel and UCSF researchers will evaluate project success criteria, identify changes in candidate health outcomes, and measure related cost savings as defined by the County. Initially, Palantir engineers will work closely with relevant end users to learn the analytical workflows required and external evaluation tools (e.g. statistical analysis software) used in concert with Palantir.

Once the workflows have been defined, Palantir engineers will train County and UCSF personnel in the execution of relevant workflows in Palantir's platform. Palantir will provide access to the aggregation features of the triage tools to enable evaluators to track the status of homeless clients and their involvement within the study. As needed, Palantir will create a clean and intuitive interface that summarizes the trends across all homeless clients involved in the study to answer specific Pay for Success outcomes.



As needed for evaluation purposes, Palantir engineers will also integrate additional data fields from the existing data sets.

**TIMELINE**

At a high level, we envision the development process occurring in multiple phases. These timelines are somewhat fungible, and some efforts may proceed concurrently.

<b>PHASE</b>	<b>DESCRIPTION</b>
<b>Pre-implementation</b> <i>(~1 month)</i>	Obtain access to key data sets and other resources for team members: <ul style="list-style-type: none"> <li>• Complete approval processes and trainings as needed</li> <li>• Establish network connections and points of contact to target systems</li> <li>• Validate and understand databases with relevant County staff</li> <li>• Complete Personnel on-boarding</li> <li>• Establish triage criteria applied with Palantir software</li> <li>• Conduct user interviews with UCSF researchers and County Study Team members</li> </ul>
<b>Data Integration</b> <i>(~4 months)</i>	Integrate data from target databases into Palantir’s platform. Database set includes: <ul style="list-style-type: none"> <li>• SCV HHS Data (HealthLink &amp; Unicare) (via direct connection or periodic extract)</li> <li>• ELMR (via direct connection or periodic extract)</li> <li>• CJIC (via direct connection or periodic extract)</li> </ul> Devise a method and criteria for linking records across data sets
<b>Triage &amp; reporting</b> <i>(~1 month)</i>	Devise a method for identifying candidates based on defined criteria: <ul style="list-style-type: none"> <li>• Implement triage method</li> <li>• Define County and UCSF researcher workflows to accessing relevant triage population information</li> <li>• If necessary, create single candidate summary view</li> </ul>
<b>Evaluation</b> <i>(~2 months)</i>	Develop processes for evaluating project success criteria, cost savings, and improved health outcomes. <ul style="list-style-type: none"> <li>• Integrate more fields from existing data sets as needed.</li> <li>• Enable analytical workflows and train Study Team in execution.</li> <li>• Leverage existing Palantir analytical capabilities and solutions.</li> </ul>

//

//

//

## GOVERNANCE

### Project Oversight

<b>ROLE</b>	<b>RESPONSIBILITIES</b>
<b>Steering Committee</b> <i>Monthly meetings</i>	Jointly govern the overall project Responsible for prioritizing project objectives, reviewing progress against milestones, and removing roadblocks Sets policies and rules for Platform access -- in accordance with all applicable laws, rules, regulations, approvals, and agreements -- including requirements for training and user consent frameworks Determine strategic direction for future projects
<b>Project Team</b> <i>Weekly meetings</i>	Responsible for day-to-day project leadership, management, and coordination Facilitates all steps of data source access brokering, network IT coordination, and documentation. Where necessary, escalates requests to Steering Committee for additional support. Provides feedback on data integration efforts (including data modeling decisions and Triage Tool development), assists in identifying potential end users for soliciting their feedback, and identifies and connects any additional subject matter experts who may be needed to support data integration and modeling engineering efforts. Regularly update the Steering Committee on project progress, roadblocks, and other pertinent issues

### County and Palantir Project Teams

In addition to the oversight roles described above, County will ensure appropriate staff are assigned to perform the following functions:

<b>ROLE</b>	<b>RESPONSIBILITIES</b>
<b>Project Lead</b>	Identify POCs with knowledge of data sources and workflows Review and engage on weekly project progress updates Ensure project is answering most relevant business questions and hypotheses Partner with Palantir team to operationalize insights

<b>Technical Lead</b>	<p>Partner with Palantir team to obtain necessary access to County data systems following completion of all legal and administrative approval processes</p> <p>Provide Palantir team with access to required data sources and data dictionaries (when available)</p> <p>Help Palantir team resolve technical issues, such as by providing access to network environment</p> <p>Coordinate with Palantir in procuring any hardware or cloud infrastructure related to this project in order to facilitate receipt of relevant information and recommendations from Palantir, as agreed upon between the parties</p>
-----------------------	--

<b>Subject Matter Experts</b>	<p>Work with the Palantir team on data modeling</p> <p>Provide feedback on methodologies</p>
-------------------------------	--

<b>Analysts and Researchers</b>	<p>Work closely alongside Palantir team to clearly define current workflows</p> <p>Provide feedback to Palantir team throughout the implementation process</p>
---------------------------------	--

Palantir will deploy a multi-disciplinary project team that brings the full force of the company to bear against the business challenge. Palantir commits to provide appropriate personnel to fill the following functional roles for the project:

<b>ROLE</b>	<b>RESPONSIBILITIES</b>
<b>Project Lead</b>	<p>Primary point of contact</p> <p>Ensures team is aligned against key outcomes</p> <p>Communicates goals, needs, and wins to Executive Sponsor and other internal stakeholders</p>
<b>Forward Deployed Engineer</b>	<p>Integrates data into environment</p> <p>Implements and deploys workflows</p> <p>Configures the software</p>
<b>Deployment Strategist</b>	<p>Works with users to appropriately model data</p> <p>Creates workflows</p> <p>Works with subject matter experts to identify value in data sets</p>
<b>Civil Liberties Engineer</b>	<p>Provides specialized knowledge and experience in developing, configuring, and deploying privacy-protective and privacy-enhancing technologies to ensure that the project complies with applicable regulatory, legal, and ethical standards and requirements.</p>

Palantir's deployment model surges staffing resources as needed and deploys all necessary engineers to achieve required outcomes for our customers. As a result, County and Palantir agree that Palantir will have the flexibility to on-board engineers and deployment strategists as needed and rotate equally capable individuals on and off the project team. Palantir will work with the County to ensure continuity at both the executive and project level throughout the term of the project.

## **ENGAGEMENT MODEL AND OPERATIONAL REQUIREMENTS**

### **Hosting**

The Platform will be implemented as a virtual private cloud infrastructure (“Palantir Cloud”). Palantir Cloud deployments are supported by Amazon Web Services.

Palantir has developed a robust security infrastructure to protect customer data that encrypts every layer of the Palantir solution, and will leverage that security infrastructure for all relevant aspects of this project. Palantir will be responsible for cloud installation and maintenance, however, the County will retain stewardship and control of the instance and data hosted therein. Specifically, as outlined in Palantir’s Master Services Agreement, the County will maintain ownership of any data or content that is provided by the County for transmission, storage, integration, import, display, distribution or use in or through use of the Platform.

### **Access**

In order to facilitate Palantir’s provision of first-class support to County personnel, the County will make best efforts to provide the Palantir project team with permanent desk space and building access at the Office of Supportive Housing for the duration of the project. County will provide Palantir with remote access to the networks and databases where possible, and in accordance with applicable protocols, agreements, restrictions, and approvals.

## EXHIBIT B

### PALANTIR SUPPORT SERVICES

1. **SUPPORT SERVICES.** Support Services consist of (a) Error Correction; (b) Technical Support provided to the Customer's technical support contact concerning the use of the Cloud Solution and Client Software; and (c) Product Major Releases and Product Updates that Palantir in its discretion makes generally available without additional charge to a Customer that is up to date on all fees due under its current Agreement (any such update will be subject to the Agreement as though it were the applicable Cloud Solution).

2. **ERROR SEVERITY LEVELS.** Palantir shall exercise commercially reasonable efforts to correct any Error reported by Customer in accordance with the Severity (also called "priority" or "P") level reasonably assigned to such Error by Palantir.

- **Severity 1 Errors** - Palantir shall promptly commence the following procedures: (i) assigning Palantir engineers or other Palantir-trained personnel to correct the Error(s); (ii) moving the production instance to a failover stack, (iii) notifying Palantir management that such Errors have been reported and of steps being taken to correct such Error(s); (iv) providing Customer with periodic reports on the status of the corrections; (v) initiating work to provide Customer with a Workaround; and (vi) if appropriate, providing Palantir engineers or other trained personnel on site at Customer's facilities.
- **Severity 2 Errors** - Palantir shall promptly commence the following procedures: (i) assigning Palantir engineers or other Palantir-trained personnel to correct the Error; (ii) initiate issue resolution, (iii) notifying Palantir management that such Errors have been reported and of steps being taken to correct such Error(s); (iv) providing Customer with periodic reports on the status of the corrections; (v) initiating work to provide Customer with a Workaround; (vi) if necessary, move the production to a failover stack; and (vii) if appropriate, providing Palantir engineers or other trained personnel on site at Customer's facilities.
- **Severity 3 Errors** - Palantir shall promptly commence the following procedures: (i) assigning Palantir engineers or other Palantir-trained personnel to correct the Error; (ii) assess the issue and devise a resolution plan, (iii) if necessary, move the production instance to a failover stack, (iv) notifying Palantir management that such Errors have been reported and of steps being taken to correct such Error(s); (v) providing Customer with periodic reports on the status of the corrections; (vi) initiating work to provide Customer with a Workaround; and (vii) if appropriate, providing Palantir engineers or other trained personnel on site at Customer's facilities.
- **Severity 4 Errors** - Palantir shall commence the following procedures during regular business hours: (i) assigning Palantir engineers or other Palantir-trained personnel to correct the Error; (ii) providing Customer with periodic reports on the status of the corrections; (iii) initiating work to provide Customer with a Workaround; and (iv) if appropriate, providing Palantir engineers or other trained personnel on site at Customer's facilities.
- **Severity 5 Errors** - Palantir may include the Fix for the Error in the next Update.

3. **RESPONSE TIMES.** Palantir will use diligent efforts to meet the following response times:

<b>Severity Level / Priority Level</b>	<b>Acknowledgement Time</b>	<b>Targeted Resolution Service Level</b>
<b>1/P0</b>	<b>15 Minutes</b>	<b>Move the production instance to a failover stack within 1 hour.</b>
<b>2/P0</b>	<b>30 Minutes</b>	<b>If the issue is not resolved within 3 hours, move the production instance to a failover stack within 1 hour.</b>
<b>3/P1</b>	<b>60 Minutes</b>	<b>If the issue is not resolved within 7 hours, move the production instance to a failover stack within 1 hour.</b>
<b>4/P2</b>	<b>10 Business Hours</b>	<b>Error resolved with Product Update</b>
<b>5/P3</b>	<b>60 Business Hours</b>	<b>Error resolved at Palantir's discretion</b>

4. EXCLUSIONS. Palantir shall have no obligation to support: (i) altered or damaged Cloud Solution or Client Software or any portion of either of the foregoing incorporated with or into other software; (ii) Cloud Solution or Client Software that is not the then-current release provided by Palantir to Customer; (iii) Cloud Solution or Client Software problems caused by Customer's negligence, abuse or misapplication, use of the Cloud Solution or Client Software other than as specified in the Palantir user manual or Documentation, or other causes beyond the control of Palantir; (iv) Cloud Solution or Client Software installed on any hardware or virtual infrastructure that is not supported by Palantir; or (v) Customer-owned or installed hardware or software; or (vi) issues arising from communications facilities, networks, and computing facilities not controlled by Palantir. Palantir shall have no liability for any changes in Customer's hardware or virtual infrastructure which may be necessary to use Cloud Solution or Client Software due to a Workaround or Update.

5. CUSTOMER OBLIGATIONS. As a prerequisite to Palantir's obligations hereunder, Customer agrees to the following obligations.

5.1 Customer will establish and maintain a qualified support team that will:

- Include personnel familiar with the environment and configuration who are trained and facile in use of the diagnostic tools provided by Palantir with the Cloud Solution or Client Software, including the ability to screen and release this information in a timely manner.
- Provide Palantir engineers with reasonable access to end-users to enable direct reporting problems or issues.
- Maintain proper functioning of end-user workstations, the Customer network, and any data transfer from the Customer network.
- Provide Palantir with appropriate access to configure and diagnose the data transfer service.

In addition, this support team must be generally available and able to collect data and report it back to Palantir within 24 to 48 hours of requests made by Palantir.

5.2 Customer will follow instructions provided by Palantir when upgrading Client Software and using Updates to the Cloud Solution. For instance, Customer will have the required versions of web browsers and java installed and appropriately configured.

6. SECURITY INCIDENTS. Customer should report suspected Security Incidents involving the Cloud Solution via email (security@palantir.com) or phone (+1 855 777 0411).

7. COMMUNICATIONS FACILITIES AND NETWORKS. Palantir will use reasonable commercial efforts to (i) notify Customer in advance of scheduled downtime of the Cloud Solution due to routine maintenance and (ii) perform such routine maintenance during non-Business Hours. The Cloud Solution requires transfer of data, information or content over communications facilities, networks, and computing facilities, including the Internet or the third-party hosting service, and may be subject to limitations, delays, and other problems inherent in the use of the foregoing. Palantir is not responsible for any delays, delivery failures, or other damage resulting from such problems or the third-party hosting service (including without limitation, uptime guarantees, outages or failures).

8. DEFINITIONS.

Capitalized terms used herein, but not defined below, shall have the meanings ascribed to them in the Agreement.

- "Acknowledgement" refers to the creation of a JIRA ticket within our configured implementation of Atlassian JIRA
- "Business Hours" means hours occurring during the period of each day in which Palantir offers Support Services 9 A.M.-8 P.M. Eastern Time.
- "Error" means an error in the Cloud Solution or Client Software that is reproduced by Palantir and which significantly degrades such Cloud Solution or Client Software as compared to the Palantir's published performance specifications.
- "Error Correction" means the use of reasonable commercial efforts to correct Errors.
- "Fix" means the repair or replacement to remedy an Error.
- "Severity 1 Error" means an Error which renders a Cloud Solution system outage or catastrophic Cloud Solution system failure.

- “Severity 2 Error” means an Error which renders the Cloud Solution inoperative or causes widespread sporadic system instability.
- “Severity 3 Error” means an Error which severely degrades the performance of the Cloud Solution or substantially restricts Customer’s use of such Cloud Solution or Client Software.
- “Severity 4 Error” means an Error which causes only a minor impact on the Customer’s use the Cloud Solution functionality.
- “Severity 5 Error” means an Error which causes only a very minor impact on the Customer’s use of the Cloud Solution, such as documentation typos or handled error messages.
- “Security Incident” means malicious activity that results or is likely to result in the compromise, damage, breach or degradation of Cloud Services.
- “Support Services” means Palantir support services as described in Section 1.
- “Technical Support” means technical support assistance provided by Palantir via email, telephone or other means provided by Palantir in its discretion to the Technical Support Contact during Palantir’s normal business hours concerning the use of the then-current release of the Cloud Solution.
- “Updates” means Cloud Solution changes that Palantir implements in the applicable generally available Cloud Solution without the payment of additional fees, and associated Client Software updates. Updates do not include new platform services that Palantir makes available for an additional charge.
- “Workaround” means a change in the procedures followed or data supplied by Customer to avoid an Error without substantially impairing Customer’s use of the Cloud Solution or Client Software.

THESE TERMS AND CONDITIONS CONSTITUTE A SERVICE CONTRACT AND NOT A PRODUCT WARRANTY. ALL SERVICES, SOFTWARE AND MATERIALS RELATED THERETO ARE SUBJECT EXCLUSIVELY TO THE WARRANTIES AND LIABILITY PROVISIONS SET FORTH IN THE AGREEMENT. THIS ATTACHMENT IS AN ADDITIONAL PART OF THE AGREEMENT AND DOES NOT CHANGE OR SUPERSEDE ANY TERM OF THE AGREEMENT EXCEPT TO THE EXTENT UNAMBIGUOUSLY CONTRARY THERETO.

## EXHIBIT C

### BUSINESS ASSOCIATE AGREEMENT

**WHEREAS**, County of Santa Clara (“County” or “Covered Entity”) is a Covered Entity, as defined below, and wishes to disclose certain Protected Health Information (“PHI”) to Palantir (which is or will be a “Business Associate” as that term is used herein) pursuant to the terms of the Agreement and this Business Associate Agreement (“BAA”); and

**WHEREAS**, the County is a hybrid entity pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) performing both covered and non-covered functions; and

**WHEREAS**, the Santa Clara Valley Health and Hospital System, which is part of the County is comprised of multiple County Departments, including Valley Medical Center and Clinics (“VMC”), the County Mental Health Department (“MHD”), the County Department of Alcohol and Drug Services (“DADS”), the County Public Health Department (“PHD”) and the County Custody Health Services (“Custody Health”) and County Valley Health Plan (“VHP”), all of which are “Covered Entities” under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”); and

**WHEREAS**, the Covered Entity and Business Associate are “qualified service organizations” or “QSO” within the meaning of the federal law governing Confidentiality of Alcohol and Drug Abuse Patient Records and its implementing regulations, 42 Code of Federal Regulations (“C.F.R.”) Part 2; and

**WHEREAS**, the Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI used and disclosed pursuant to this BAA in compliance with HIPAA, the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (“the HITECH Act”), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the “HIPAA Regulations”), California Welfare & Institutions Code 5328, 42 U.S.C. Section 290dd-2, 42 C.F.R. part 2, California Confidentiality of Medical Information Act Civil Code Section 56, California Health & Safety Code 1280.15, and other applicable laws; and to the extent the Business Associate is to carry out the Covered Entity’s obligation under the Privacy Rule, the Business Associate must comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligation.

**WHEREAS**, part of the HIPAA Regulations, the Privacy Rule and the Security Rule (defined below) require Covered Entities to enter into a contract containing specific requirements with any Business Associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e) and 164.504(e) of the Code of Federal Regulations (“C.F.R.”) and contained in this BAA.

**NOW, THEREFORE**, in consideration of the mutual promises below and the exchange of information pursuant to the BAA, the parties agree as follows:

#### **I. Definitions**

Terms used, but not otherwise defined, and terms with initial capital letters in the BAA have the same meaning as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005, and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the “HIPAA Regulations”) and other applicable laws.

**Breach** Any acquisition, access, use or disclosure of Protected Health Information in a manner not permitted or allowed under state or federal privacy laws.

**Business Associate** is a person, organization, or agency other than a workforce member that provides specific functions, activities, or services that involve the use, creation, or disclosure of PHI for, or on behalf of, a HIPAA covered health care component. Examples of business associate functions are activities such as claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, repricing; and legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.



**Contract** means the Agreement to which this Business Associate Agreement is appended as an exhibit, and **Addendum** means any addendum, amendment or supplement thereto.

**Covered Entity** shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103.

**Designated Record Set** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

**Electronic Protected Health Information** means Protected Health Information that is maintained in or transmitted by electronic media.

**Electronic Health Record** shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921.

**Health Care Operations** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

**Privacy Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.

**Protected Health Information or PHI** means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an Individual; the provision of health care to an Individual; or the past, present or future payment for the provision of health care to an Individual; and (ii) that identifies the Individual or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 160.103. Protected Health Information includes Electronic Protected Health Information [45 C.F.R. Sections 160.103, 164.501].

**Protected Information** shall mean PHI provided by Covered Entity to Business Associates or created or received by Business Associates on Covered Entity's behalf.

**Security Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

**Unsecured PHI** shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h)(1) and 45 C.F.R. 164.402.

## **II. Duties & Responsibilities of Business Associates**

- a. Permitted Uses.** Business Associate shall use Protected Information only for the purpose of performing Business Associate's obligations under the Contract and as permitted or required under the Contract or Addendum, or as required by law. Further, Business Associate shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule, Welfare & Institutions Code Section 5328, 42 C.F.R. Part 2, or the HITECH Act, if so used by Covered Entity. However, Business Associate may use Protected Information (i) for the proper management and administration of Business Associate, (ii) to carry out the legal responsibilities of Business Associate, or (iii) for Data Aggregation purposes for the Health Care Operations of Covered Entity. [45 C.F.R. Sections 164.502(a)(3), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(i)]
- b. Permitted Disclosures.** Business Associate shall not disclose Protected Information except for the purpose of performing Business Associate's obligations under the Agreement and as permitted under the Agreement and this BAA. Business Associate shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule, 42 C.F.R., Welfare & Institutions Code Section 5328, or the HITECH Act if so disclosed by Covered Entity. However, Business Associates may disclose Protected Information (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business

Associate; (iii) as required by law; or (iv) for Data Aggregation purposes for the Health Care Operations of Covered Entity. If Business Associate discloses Protected Information obtained pursuant to the Agreement and this BAA to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such Protected Information will be held confidential as provided pursuant to this BAA and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to notify Business Associate of any Breaches of confidentiality of the Protected Information within the timeframe required by 45 C.F.R. 164.410, to the extent it has obtained knowledge of such Breach. [42 U.S.C. Section 17932; 45 C.F.R. Sections 164.504(e)(2) (i)-(ii)(A) and 164.504(e)(4)(ii)].

- c. **Prohibited Uses and Disclosures.** Business Associate shall not use or disclose Protected Information for fundraising or marketing purposes. [42 U.S.C. Section 17936(a) and 45 C.F.R. 164.501]. Business Associate shall not disclose Protected Information to a health plan for payment or health care operations purposes if the Individual has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates. [42 U.S.C. Section 17935(a); 45 C.F.R. Section 164.502(a)(5)(ii)]. Business Associate shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of Covered Entity and as permitted by the HITECH Act. [42 U.S.C. Section 17935(d)(2)]. This prohibition shall not affect payment by Covered Entity to Business Associate for services provided pursuant to the Agreement.
- d. **Appropriate Safeguards.** Business Associate shall implement appropriate administrative, technological and physical safeguards as are necessary to prevent the use or disclosure of Protected Information other than as permitted by this BAA that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Information, and comply, where applicable, with the HIPAA Security Rule with respect to Electronic PHI.
- e. **Reporting of Improper Access, Use or Disclosure.** Business Associate shall report to Covered Entity in writing any access, use or disclosure of Protected Information not permitted by the Agreement and BAA, and any Breach of Unsecured PHI of which it becomes aware without unreasonable delay and in no case later than 10 calendar days after its discovery of such event [42 U.S.C. Section 17921; 45 C.F.R. Section 164.504(e) (2) (ii) (C); 45 C.F.R. Section 164.308(b)]. All reports to Covered Entity pursuant to this section shall be sent to the Covered Entity Compliance Officer by facsimile and U.S. mail using the following contact information:

Compliance & Privacy Officer  
Santa Clara Valley Health & Hospital System  
2325 Enborg Lane, Suite 240  
San Jose, CA 95128  
Facsimile (408) 885-6886  
Telephone (408) 885-3794

The breach notice must contain: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known, (2) the location of the breached information; (3) a description of the types of PHI that were involved in the breach, (4) Safeguards in place prior to the breach; (5) Actions taken in response to the breach; (6) any steps individuals should take to protect themselves from potential harm resulting from the breach, (7) a brief description of what the business associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches, and (8) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website or postal address. [45 C.F.R Section 164.410] Business Associate shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

- f. **Business Associate's Agents and Subcontractors.** Business Associate shall ensure that any agents or subcontractors, to whom it provides Protected Information, agree in writing to the same restrictions and conditions that apply to Business Associate with respect to such PHI and implement the safeguards required by paragraph (II) d above with respect to Electronic PHI. [45

C.F.R. Sections 164.502(e)(1)(ii), 164.504(e)(2)(ii)(D) and 164.308(b)]. If Business Associate knows of a pattern of activity or practice of an agent or subcontractor that constitutes a material breach of violation of an agent or subcontractor's obligations under the Contract or Addendum or other arrangement, the Business Associate must take reasonable steps to cure the breach or end the violation. If these steps are unsuccessful, Business Associate shall terminate the contract or arrangement with agent or subcontractor, if feasible. [45 C.F.R. Section 164.504(e)(1)(iii)]. Business Associate shall provide written notification to Covered Entity of any pattern of activity or practice of a subcontractor or agent that Business Associate believes constitutes a material breach or violation of the agent or subcontractor's obligations under the Contract or Addendum or other arrangement with twenty four (24) hours of discovery and shall meet with Covered Entity to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

The Business Associate shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation.

For the purposes of this BAA, the parties hereby agree that if Business Associate utilizes the services of Amazon Web Services, it will do so pursuant to Business Associate Agreement between Business Associate and Amazon Web Services that complies with all applicable laws, rules, and regulations, including HIPAA.

- g. Access to Protected Information.** Business Associate shall make Protected Information maintained by Business Associate or its agents or subcontractors in Designated Record Sets available to Covered Entity for inspection and copying within ten (10) days of a request by Covered Entity to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524. [45 C.F.R. Section 164.504(e)(2)(ii) (E); 42 C.F.R. part 2 and Welfare & Institutions Code Section 5328]. If Business Associate maintains an Electronic Health Record, Business Associates shall provide such information in electronic format to enable Covered Entity to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. Section 17935(e)(1). If any Individual requests access to PHI directly from Business Associate or its agents or subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the request.
- h. Electronic PHI.** If Business Associate receives, creates, transmits or maintains Electronic PHI on behalf of Covered Entity, Business Associate will, in addition, do the following:
- (1) Develop, implement, maintain and use appropriate administrative, physical, and technical safeguards in compliance with Section 1173(d) of the Social Security Act, Title 42, Section 1320(s) or the United States Code and Title 45, Part 162 and 164 of CFR to preserve the integrity and confidentiality of all electronically maintained or transmitted PHI received from or on behalf of Covered Entity.
  - (2) Document and keep these security measures current and available for inspection by Covered Entity.
  - (3) Ensure that any agent, including a subcontractor, to whom the Business Associate provides Electronic PHI, agrees to implement reasonable and appropriate safeguards to protect it.
  - (4) Report to the Covered Entity any Security Incident of which it becomes aware. For the purposes of this BAA and the Agreement, Security Incident means, as set forth in 45 C.F.R. Section 164.304, "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." Security incident shall not include, (a) unsuccessful attempts to penetrate computer networks or servers maintained by Business Associate, or (b) immaterial incidents that occur on a routine basis, such as general "pinging" or "denial of service" attacks.
- i. Amendment of PHI.** Within ten (10) days of receipt of a request from Covered Entity for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, Business Associate or its agents or subcontractors shall make such Protected

Information available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under the Privacy Rule. If any Individual requests an amendment of Protected Information directly from Business Associate or its agents or subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of the request. Any approval or denial of amendment of Protected Information maintained by Business Associate or its agents or subcontractors shall be the responsibility of Covered Entity.

- j. **Accounting Rights.** Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with Privacy Rule and the HITECH Act. [42 U.S.C. Section 17935(c) and 45 C.F.R. Section 164.528]. Business Associate agrees to implement a process that allows for an accounting of disclosures to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years prior to the request. Accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for three (3) years prior to the request, and only to the extent Business Associate maintains an electronic health record and is subject to this requirement.

At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed and (iv) a brief statement of purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure. [45 C.F.R. Section 164.528(b)]. In the event that the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, Business Associate shall forward it to Covered Entity in writing within five (5) days of the request. It shall be Covered Entity's responsibility to prepare and deliver any such accounting requested. Business Associate shall not disclose any Protected Information except as set forth in the Agreement and this BAA.

- k. **Governmental Access to Records.** Business Associate shall make its internal practices, books and records relating to the use and disclosure of Protected Information available to Covered Entity and to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for purposes of determining Business Associate's compliance with the Privacy Rule [45 C.F.R. Section 165.504(e)(2)(ii)(I)]. Business Associate shall concurrently provide to Covered Entity a copy of any internal practices, books, and records relating the use and disclosure of PHI that Business Associate provides to the Secretary.
- l. **Minimum Necessary.** Business Associate and its agents or subcontractors shall request, use and disclose only the minimum amount of Protected Information reasonably necessary to accomplish the purpose of the request, use, or disclosure in accordance with 42 U.S.C. Section 17935(b). Business Associate understands and agrees that the definition of "minimum necessary" is defined in HIPAA and may be modified by the Secretary. Each party has an obligation to keep itself informed of guidance issued by the Secretary with respect to what constitutes "minimum necessary."
- m. **Adherence to the Requirements of 42 C.F.R.** Business Associate acknowledges that in receiving, transmitting, transporting, storing, processing or otherwise dealing with patient records and information in connection with providing drug testing services to patients covered by SCVHHS under this Agreement and BAA, it is fully bound by the regulations governing confidentiality of alcohol and drug abuse patient records, 42 C.F.R. Section 2.1, *et seq.*, and HIPAA, and may not use or disclose the information except as permitted or required by this BAA or applicable law.
- n. **Resist Efforts in Judicial Procedures.** Business Associates agree to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Records, 42 C.F.R. Part 2.
- o. **Data Ownership.** Business Associate acknowledges that Business Associate has no ownership rights with respect to the Protected Information governed by this BAA, and all rights, interests, and title remain vested in the County at all times.

### III. Termination

- a. **Material Breach.** A breach by Business Associate of any provision of this BAA shall constitute a material breach of the Agreement and shall provide grounds for immediate termination of the Agreement if such breach is uncured by Business Associate within thirty (30) days of receiving notice from Covered Entity of such breach, any provision in the Agreement to the contrary notwithstanding. [45 C.F.R. Section 164.504(e)(2)(iii)].
- b. **Judicial or Administrative Proceedings.** Covered Entity may terminate the Agreement, effective immediately, if (i) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, 42 C.F.R. Part 2, the HIPAA Regulations or other security or privacy laws or (ii) a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, the HITECH Act, 42 C.F.R. Part 2, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.
- c. **Effect of Termination.** Upon termination of the Agreement for any reason, Business Associate shall, at the option of Covered Entity, return or destroy all Protected Information that Business Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, Business Associate shall continue to extend the protections of Section 2 of the BAA to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. [45 C.F.R. Section 164.504(e) (ii)(2)(1)]. If County elects destruction of the PHI, Business Associate shall certify in writing to County that such PHI has been destroyed.

### IV. General Provisions

- a. **Indemnification.** In addition to the indemnification language in the Agreement, Business Associate agrees to be responsible for, and defend, indemnify and hold harmless the Covered Entity for any breach of Business Associate's privacy or security obligations under the Agreement, including any fines, penalties and assessments that may be made against Covered Entity or the Business Associate for any Breaches or late reporting and agrees to pay the cost of and notice for any credit monitoring services only to the extent that such Breach results from (i) the failure of Business Associate to perform in accordance with the terms of the Agreement, the Business Associate Agreement, and/or Business Associate's then-current documentation, or (ii) negligence or willful misconduct on the part of Business Associate's employees or agents.
- b. **Disclaimer.** Covered Entity makes no warranty or representation that compliance by Business Associate with this BAA, HIPAA, the HITECH Act, or the HIPAA Regulations will be adequate or satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decisions made by Business Associate regarding the use and safeguarding of PHI.
- c. **Amendment to Comply with Law.** The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the Agreement or BAA may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable California laws relating to the security or confidentiality of PHI.
- d. Upon the request of any party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to the BAA embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable California laws relating to the security or confidentiality of PHI.
- e. **Assistance in Litigation of Administrative Proceedings.** Unless prohibited by law, Business associate shall promptly notify Covered Entity of any litigation or administrative proceedings commenced against Business Associate arising from the performance of its obligations under the Agreement or BAA.

- f. No Third-Party Beneficiaries.** Nothing express or implied in the Agreement or this BAA is intended to confer, nor shall anything herein confer, upon any person other than Covered Entities, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.
- g. Effect on Agreement.** Except as specifically required to implement the purposes of the BAA, or to the extent inconsistent with this BAA, all other terms of the Agreement shall remain in force and effect.
- h. Interpretation.** The BAA shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule. The parties agree that any ambiguity in this BAA shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, 42 Code of Federal Regulations ("C.F.R.") Part 2, the Privacy Rule and the Security Rule and other applicable California laws relating to the security or confidentiality of PHI.
- i. Governing Law, Venue.** This agreement has been executed and delivered in, and shall be construed and enforced in accordance with, the laws of the State of California. Proper venue for legal action regarding this Agreement shall be in the County of Santa Clara.
- j. Survivorship.** The respective rights and responsibilities of Business Associate related to the handling of PHI survive termination of this Agreement.

