

## MASTER SUBSCRIPTION AGREEMENT NO. 230173B

THIS MASTER SUBSCRIPTION AGREEMENT (“**Agreement**”) is entered into by and between Collective Medical Technologies, Inc., a PointClickCare company (“**Collective**”) and Napa County Health and Human Services Agency (“**Subscriber**”) (each a “**Party**” and, collectively, the “**Parties**”), each on behalf of itself and its Affiliates, and is effective as of 2/1/2023 (the “**Effective Date**”). In consideration of the mutual promises and covenants contained herein, and for other good and valuable consideration, the receipt, sufficiency, and adequacy of which are hereby acknowledged, the Parties hereby agree as follows:

### 1. Certain Definitions

- 1.1. “**Affiliate**” means any organization (a) which controls, is controlled by, or is under common ownership or control with a Party; or (b) for which a Party directly or indirectly holds or controls fifty percent (50%) or more of the beneficial ownership or voting interest or the power to direct or cause the direction of the management or policies of an entity, whether through the ability to exercise voting power, by contract, or otherwise.
- 1.2. “**Authorized Purposes**” are the purposes and activities for which Subscriber authorizes Collective, and for which Subscriber is authorized, to use or disclose Patient Data through the Services, which are treatment, payment, health care operations and public health activities, as those terms are used and defined in 45 C.F.R. §§ 160 and 164, and in all cases only as permitted by applicable state and federal law.
- 1.3. “**BAA**” means the Business Associate Agreement executed by and between the Parties, attached hereto as Attachment B.
- 1.4. “**Collective Network**” means the network facilitated by the Collective Platform pursuant to which Network Participants share Patient Data for Authorized Purposes.
- 1.5. “**Collective Platform**” means certain remotely hosted software-as-a-service (SaaS) applications and their underlying technologies that facilitate access to information sourced from Network Participants on the Collective Network.
- 1.6. “**Network Participant**” means (i) a Partner Network or (ii) any covered entity, business associate, or other health care entity that participates in the Collective Network by executing an agreement with Collective with network terms substantially similar to those set forth in this Agreement. Subscriber is a Network Participant.
- 1.7. “**Network Policies**” means the Network Security Policy, the applicable Sensitive Information Policy, the Terms of Use, the System Requirements, and such other Collective-defined policies and requirements available or referenced at <https://collectivemedical.com/network-policies/> which govern the technical or administrative operations of the Collective Network and which may be updated or amended by Collective in accordance with Section 11.6, below.
- 1.8. “**Partner Network**” means a data solutions provider or electronic data exchange network (such as a health information exchange or an electronic medical record with interoperability functionality for sharing Patient Data) with which Collective has a relationship which allows sharing of certain Patient Data for Authorized Purposes.
- 1.9. “**Patient Data**” has the same meaning as the term “protected health information” in 45 C.F.R. § 160.103, but, where context dictates, limited to the information created or received by Collective from or on behalf of Subscriber.
- 1.10. “**Sensitive Information**” is a subset of Patient Data which is specifically identified or referred to in the Sensitive Information Policy and which includes, but is not limited to, Psychotherapy Notes and Substance Use Disorder Information.
- 1.11. “**Service Levels**” means the service levels set forth in Attachment A.
- 1.12. “**Service Order Form**” or “**SOF**” means an ordering document specifying the Services to be provided hereunder that is entered into between Subscriber and Collective, including any addenda and supplements

thereto. SOFs shall be deemed incorporated herein by reference. No SOF will be binding unless executed by both Parties.

- 1.13. “**Services**” means the provision of access to and participation in the Collective Network via one or more SaaS applications on the Collective Platform, including updates and modifications thereto, related support services, configurations, implementations, documentation, and training services, in each case as specified in a SOF.
- 1.14. “**Terms of Use**” or “**ToU**” means the terms of use for the Services, available at <https://collectivemedical.com/collective-policies/> or such other URL as Collective may provide.
- 1.15. “**Users**” means any of Subscriber’s employees, agents, workforce members, and independent contractors which Subscriber authorizes to use the Services in accordance with the Agreement, including the Terms of Use.

## 2. **Services.**

- 2.1. **Subscription.** Subject to the terms of the Agreement and any restrictions set forth in a SOF, Collective grants Subscriber and its Users a non-exclusive, non-transferable, non-sublicenseable right to have its Users: (a) access the features and functions of the Services ordered under a SOF solely for Subscriber’s internal business purposes; and (b) view, download and use the content made available to Subscriber and Users through the Services solely in accordance with the terms of this Agreement. Subscriber and Users will use the Services in accordance with the ToU. Except as expressly set forth in this Agreement, Collective retains all right, title and interest in and to the Services, and all intellectual property rights therein. Collective reserves all rights not expressly granted to Subscriber under this Agreement.
- 2.2. **Users.** Subscriber shall grant and revoke User authorizations in accordance with Collective’s reasonable security and user-credentialing requirements as may be communicated by Collective from time to time. Subscriber shall ensure that its Users’ access to and use of the Services are in accordance with the ToU. Subscriber is solely responsible for each of its Users’: (a) use of the Services, (b) training, (c) compliance with the ToU, and (d) compliance with applicable state and federal privacy laws (including, without limitation, the HIPAA minimum-necessary standard described in 45 C.F.R. §§ 164.502(b) and 164.514(d) (the “**Minimum-Necessary Standard**”).
- 2.3. **Restrictions.** Subscriber and its Users may use the Services only in accordance with applicable law and the Agreement. Except as expressly authorized by the Agreement, Subscriber will not, and will not allow any User or other third party under its control to, (a) permit any non-User to access or use the Services; (b) decompile, disassemble, reverse engineer, or otherwise attempt to derive the trade secrets embodied in the Services; (c) use the Services or any Collective Confidential Information to develop a competing product or service or create any derivative works based on the Services; (d) use any Services, or allow the transfer, transmission, export, or re-export of any Services or portion thereof in violation of any export control laws or regulations administered by the U.S. Commerce Department or any other government agency; (e) bypass or breach any security device or protection used by the Services or access or use the Services other than through the use of a User’s own then-valid access credentials; (f) input, upload, transmit, or otherwise provide to or through the Services any information or materials that are unlawful or injurious or which contain, transmit, or activate any harmful or destructive code; (g) remove any copyright, trademark, proprietary rights, disclaimer, or warning notice included on or embedded in any part of the Services, including any screen displays, etc., or any other products or materials provided by Collective hereunder; or (h) access the Services or allow any employee, contractor or agent to access the Services, with, for example, any automated or other process such as screen scraping, by using robots, web-crawlers, spiders or any other sort of bot or tool, for the purpose of extracting data, monitoring availability, performance, functionality, or for any other benchmarking or competitive purpose. Except to the extent expressly warranted by Collective hereunder, Collective will not be liable to Subscriber or otherwise responsible for any results obtained or derived by Subscriber’s use of the Services. Subscriber further acknowledges and understands that the full availability of certain functionality or content of the Services depends, in part, upon the accuracy and completeness of the Patient Data provided by Subscriber to Collective via the Services. Accordingly, such unavailability of the Services shall not be deemed to be a failure by Collective to provide the Services hereunder. Subscriber agrees that it shall hold Collective harmless from any and all adverse expenses, damages, or losses which may result from any such unavailability of the Services.

- 2.4. Connectivity; Service Levels. As between Collective and Subscriber, Subscriber is solely responsible for all telecommunication and internet connections required to access the Services, as well as all hardware and software at Subscriber's site(s). In addition to other third-party costs that may apply, Subscriber agrees to pay for all telecommunications services required for Subscriber and its Users to access the Services. Subscriber's access to the Services is conditioned upon Subscriber's compliance with the Minimum System Requirements. Collective hereby disclaims all liabilities and makes no warranties of any kind with respect to Subscriber's use of products or services provided by a third party to access or use the Services (e.g., computers, operating systems, internet connections, EMRs (if applicable), etc.). Subject to Subscriber's compliance with the terms of this Agreement, including the Minimum System Requirements, Collective shall provide the Services in accordance with the applicable Service Levels.
- 2.5. Services Ownership and Feedback. Except for the limited rights expressly provided to Subscriber herein, Collective retains all rights, title, and interest (including, without limitation, all patent, copyright, trademark, trade secret, and other intellectual property rights) in and to the Services, and all copies, modifications, and derivative works thereof (including any changes which incorporate any of Subscriber's or a User's ideas, feedback, or suggestions). Subscriber acknowledges and understands that Subscriber is obtaining only a limited right to access the Services during the Term and that, irrespective of any use of terms such as "purchase" or "sale" hereunder or in any SOF, no ownership rights are conveyed to Subscriber under the Agreement. Subscriber acknowledges that Collective makes available to all of its Network Participants on a regular basis improvements to the Services which may be based in whole or in part on feedback provided by its Network Participants and their Users and Subscriber hereby grants, to the extent Subscriber has the authority to so grant, to Collective a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into the Services any suggestion, enhancement request, recommendation, correction, or other feedback which is provided to Collective by Subscriber or its Users.
- 2.6. Subscriber Ownership of Patient Data. Subscriber shall retain ownership of its Patient Data but acquires no right, title, or interest, except for the limited right expressly granted to Subscriber herein, in Collective's proprietary format or display of same. Subscriber hereby grants to Collective a non-exclusive license to use and disclose the Patient Data that Subscriber transmits via the Services and the other data described herein, in each case solely for the purposes expressly set forth herein.

### 3. **Data Use and Compliance.**

- 3.1. Subscriber Attestation. Subscriber acknowledges and understands that the Services include certain software applications that enable Subscriber and its Users to access and share information, including Patient Data, electronically with other Network Participants for Authorized Purposes. Accordingly, in order to access the Services and participate in the Collective Network, Subscriber hereby attests that Subscriber is either a covered entity or a business associate to one or more covered entities (or both), as those terms are used and defined at 45 CFR 160.103. Collective's willingness to provide access to the Services is conditioned upon Subscriber's attestation in this Section. Subscriber shall provide additional clarifications regarding such status upon Collective's request. Any misrepresentation of such status by Subscriber shall be an incurable breach of this Agreement.
- 3.2. Business Associate. The Parties acknowledge that Collective is a business associate of Subscriber and the Services are provided subject to the BAA.
- 3.3. Network Security. Collective and Subscriber each agree to maintain administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Patient Data as required by the HIPAA Security Rule set forth at 45 CFR Part 160 and 45 CFR 164 Subparts A and C, and to comply with the Network Security Policy. Collective shall store Subscriber's Patient Data solely within the United States and shall access Subscriber's Patient Data solely from within the United States and Canada.
- 3.4. Sensitive Information Compliance. Subscriber and its Users may use and disclose Sensitive Information via the Services only to the extent that such use and disclosure are strictly in accordance with the Sensitive Information Policy.
- 3.5. Use & Disclosure of Information by Subscriber and Subscriber's Contractors.
  - 3.5.1. Subject to the terms of this Agreement, Subscriber may use and disclose Patient Data via the Services for the Authorized Purposes. As between Subscriber and Collective, Subscriber is solely

responsible for ensuring that Subscriber's use and disclosure of Patient Data via the Services (a) is limited to Authorized Purposes; (b) is permissible under any applicable notice of privacy practices; (c) is not required to be authorized or consented to by any person, including any individual to whom it pertains, or if authorization or consent of any person is required, that it has been obtained, including any consent requirements set forth in the Sensitive Information Policy; (d) is not subject to an agreed upon or required restriction which would prohibit the disclosure; and (e) is limited to individuals with whom Subscriber has a direct or indirect relationship for treatment, payment, or health care operations purposes, or for whom Subscriber is permitted by applicable law to access Patient Data for a public health purpose. Furthermore, Subscriber hereby represents that its access to, use of, and disclosure of Patient Data via the Services shall be consistent with all applicable federal and state laws, including, without limitation, the Minimum-Necessary Standard.

- 3.5.2. If Subscriber engages an individual or entity as a business associate of Subscriber to provide services on Subscriber's behalf which services require access to Patient Data via the Services (each a "**Contractor**"), Subscriber shall restrict such Contractor's use and disclosure of Patient Data to the applicable Authorized Purposes and in all cases consistent with the Minimum-Necessary Standard. To the extent that Subscriber requests that Collective directly deliver Subscriber's Patient Data to Subscriber's Contractor, via the Services or otherwise, and Collective agrees to do so, then Subscriber shall deliver an authorization letter to Collective which identifies the specific subset of Patient Data necessary to fulfill the request. Such authorization letter shall be deemed to include the following Subscriber representations: (a) that Subscriber has executed a services contract and a valid HIPAA business associate agreement with the Contractor; (b) that the Patient Data which Subscriber instructs Collective to deliver to the Contractor is consistent with the Authorized Purposes and with the Minimum-Necessary Standard; (c) that the Contractor has provided Subscriber with assurances to Subscriber's reasonable satisfaction with respect to the Contractor's information-security practices and related compliance, and that Subscriber understands and acknowledges that Collective will not be performing its own security or compliance assessments of the Contractor; (d) that Subscriber will not hold Collective responsible for the Contractor's use or disclosure of, or changes to, the Patient Data or for any other activity of Subscriber's Contractor; and (e) that Subscriber will immediately notify Collective upon termination of Subscriber's services contract or business associate agreement with the Contractor or upon any change of the scope of such agreements such that a change to the Contractor's access to Subscriber's Patient Data is merited.
- 3.5.3. State PDMP Data. To the extent that a SOF indicates that the Services include data from one or more states' prescription drug monitoring programs ("**PDMP Data**"), Subscriber's access to and use of such PDMP Data may be subject to certain additional flow-down terms and conditions imposed by the applicable state PDMP administrators, which additional terms and conditions shall be set forth in the applicable SOF.
- 3.6. Use and Disclosure of Patient Data by Collective and other Network Participants. Unless separately agreed to between Subscriber and a Network Participant, and subject to any other applicable legal or contractual requirements, obligations, limitations, or conditions, including but not limited to those set forth in this Agreement, the transfer of Patient Data by Subscriber via the Services, either directly or by way of a third party, conveys to Collective and to the Network Participants full rights to use and disclose such Patient Data for all of the Authorized Purposes, even if the original transfer of such Patient Data was made in connection with only a subset of the Authorized Purposes. Authorized Purposes may, by way of illustration and not limitation, consist of uses or disclosures of Patient Data for population health services, data aggregation services as defined in 45 C.F.R. § 164.501 and as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B), inclusion in records, disclosure to other parties, modification, de-identification in accordance with 45 C.F.R. §§ 164.502(d) and 164.514(a)-(c), and destruction, in each case only to the extent permitted by applicable law. For the avoidance of doubt, this Agreement does not permit any sale or marketing of Patient Data.
- 3.7. Use and disclosure of Patient Data by Collective. Collective may use and disclose Patient Data (i) for the Authorized Purposes as described in Section 3.6, (ii) for Collective's proper management and administration, (iii) for development and improvement of the Services, (iv) for de-identification in accordance with 45 C.F.R. §§ 164.502(d) and 164.514(a)-(c), (v) to create and share Limited Data Sets in accordance with 45 CFR § 164.514, and (vi) as otherwise authorized in this Agreement or the BAA. Any

obligation in the Agreement or the BAA to return or destroy Patient Data following termination of the Agreement or the BAA shall be understood to not apply to any Patient Data for which return or destruction is not feasible. Subscriber acknowledges that among the possible reasons for which return or destruction of Patient Data may not be feasible are instances where the Patient Data has been transmitted via the Collective Network to another Network Participant for Authorized Purposes as described herein and where Collective, therefore, holds such Patient Data pursuant to a separate HIPAA business associate agreement between Collective and such Network Participant.

3.8. Use and disclosure of Administrative Data, Transaction Data, and Derived Data by Collective.

- 3.8.1. Administrative Data. “**Administrative Data**” means information identifying and pertaining to Subscriber and its Users, such as User contact information, but which does not contain Patient Data or Subscriber’s Confidential Information, which Collective uses to manage and administer the Services and provide support to Subscriber and its Users. Collective may use and disclose Administrative Data for purposes of providing the Services to Network Participants, for the purposes set forth in the Terms of Use, for Collective’s proper management and administration, and as required by law.
- 3.8.2. Transaction Data. “**Transaction Data**” means information and statistics about Subscriber’s interactions with and usage of the Services, but which does not contain Patient Data, Administrative Data, or Subscriber’s Confidential Information. Collective may use and disclose Transaction Data for any lawful purpose, including, by way of illustration and not limitation, (i) for the analysis, development, improvement, and provision of the Services and other Collective products and services; (ii) for recordkeeping, fee calculation, internal reporting, support, and other internal business purposes; (iii) to report the number and type of transactions and other statistical information concerning the Services; and (iv) to otherwise administer and facilitate the Services.
- 3.8.3. Derived Data. “**Derived Data**” means any data that Collective derives from Patient Data, Administrative Data, or Transaction Data that does not include Subscriber’s Confidential Information or any Patient Data or other personally identifiable information. Subscriber hereby acknowledges and agrees that the Derived Data is owned by, and is the exclusive property of Collective, and that Collective may use, disclose, market, license, distribute, sell, receive remuneration for, create derivative works of, and otherwise commercialize the Derived Data for any legally permissible purpose without restriction.

4. **Fees and Payment**

- 4.1. Subscription Fees. Subscriber shall pay all fees specified in the applicable SOFs, as modified from time to time pursuant to Section 4.3 below. Except as otherwise specified herein or in a SOF, (a) fees are based on Services purchased and not actual usage, and (b) payment obligations are non-cancelable and fees paid are non-refundable.
- 4.2. Invoicing and Payment. Fees shall be invoiced in advance and otherwise in accordance with the relevant SOF. Unless otherwise stated in the SOF, fees are due net thirty (30) days from the receipt of invoice date, provided that if an invoice is sent electronically to the email address provided by Subscriber for billing, then it shall be deemed received by Subscriber as of the date it was sent. Collective shall submit invoices to Subscriber as set forth on the signature page hereof.
- 4.3. Fee Increases. Fees, or the PMPM rates used to calculate the fees, if applicable, shall increase annually by the greater of five percent (5%) or the U.S. Consumer Price Index for All Urban Consumers (CPI-U) as published by the United States Bureau of Labor Statistics over the previous year’s fees or PMPM rates, as the case may be. Additionally, Collective may increase the fees payable by Subscriber as follows: (a) in accordance with the fee provisions set forth on the applicable SOF; (b) in proportion to the increase in Subscriber’s emergency department visits, to the extent that such visits are used to calculate the fees associated with the Services, upon no less than thirty (30) days written notice; or (c) otherwise for an upcoming Renewal Term (defined in Section 9) by providing one hundred twenty (120) days written notice to Subscriber.
- 4.4. Overdue Charges. Subject to Section 4.6, if any invoiced amount is not received by Collective by the due date, then without limiting Collective’s rights or remedies, those charges may accrue late interest at the

rate of 1.5% of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower.

- 4.5. Suspension of Service. Subject to Section 4.6, if any charge owing by Subscriber is thirty (30) days or more overdue, Collective may, without limiting its other rights and remedies, suspend Services until such amounts are paid in full, provided Collective has given Subscriber at least ten (10) days' prior notice that its account is overdue and provided that Collective shall, at all times, continue to securely maintain Subscriber's Patient Data in accordance with the BAA and shall continue to make all such Patient Data available to and useable by Subscriber until such time as Collective returns or destroys such Patient Data in accordance with the BAA.
- 4.6. Payment Disputes. Collective shall not exercise its rights under Sections 4.4 (Overdue Charges) or 4.5 (Suspension of Service) if Subscriber is disputing the applicable charges reasonably and in good faith and is cooperating diligently to resolve the dispute.
- 4.7. Taxes. Collective's fees do not include any taxes, levies, duties or similar governmental assessments of any nature, including, for example, value-added, sales, use or withholding taxes, assessable by any jurisdiction whatsoever (collectively, "**Taxes**"). Subscriber is responsible for paying all Taxes associated with its purchases hereunder. If Collective has, or is later determined to have, the legal obligation to pay or collect Taxes for which Subscriber is responsible under this Section 4.7, Collective shall invoice Subscriber and Subscriber shall pay that amount unless Subscriber provides Collective with a valid tax exemption certificate which is authorized by the appropriate taxing authority.
- 4.8. Future Functionality. Subscriber agrees that its purchases are not contingent on the delivery of any future functionality or features, or dependent on any oral or written public comments made by Collective regarding future functionality or features.
5. **DISCLAIMERS**. EXCEPT AS EXPRESSLY SET FORTH HEREIN, THE SERVICES ARE PROVIDED ON AN AS-IS BASIS ONLY. WITHOUT IN ANY WAY LIMITING THE GENERALITY OF THE FOREGOING, COLLECTIVE DOES NOT REPRESENT OR WARRANT THAT THE SERVICES WILL MEET THE REQUIREMENTS OF ANY PERSON OR WILL OPERATE ERROR-FREE OR CONTINUOUSLY, AND COLLECTIVE MAKES NO OTHER REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OR REPRESENTATIONS CONCERNING MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SUBSCRIBER AGREES THAT COLLECTIVE HAS MADE NO AGREEMENTS, REPRESENTATIONS, OR WARRANTIES OTHER THAN THOSE EXPRESSLY SET FORTH IN THIS AGREEMENT, AND THAT NO OTHER STATEMENT ABOUT THE INFORMATION OR SERVICES PROVIDED UNDER THIS AGREEMENT SHALL BE DEEMED TO BE A WARRANTY EXCEPT TO THE EXTENT EXPRESSLY STATED AS SUCH A WARRANTY IN A MUTUALLY EXECUTED AMENDMENT TO THIS AGREEMENT. THE INFORMATION AVAILABLE THROUGH THE SERVICES DOES NOT REPRESENT COLLECTIVE'S RECOMMENDATIONS. SUBSCRIBER ACKNOWLEDGES THAT THE SERVICES ARE NOT DESIGNED OR INTENDED TO BE RELIED UPON IN ANY ENVIRONMENT IN WHICH THE UNAVAILABILITY OF THE SERVICES COULD LEAD TO DEATH, PERSONAL INJURY, OR PHYSICAL OR ENVIRONMENTAL DAMAGE. COLLECTIVE ASSUMES NO RESPONSIBILITY FOR THE ACCURACY, UP-TO-DATE STATUS, OR COMPLETENESS OF THE PATIENT DATA, NOR FOR SUCH PATIENT DATA'S SUFFICIENCY WITH ANY LEGAL STANDARD. SUBSCRIBER ALSO ACKNOWLEDGES AND AGREES THAT THE SERVICES AND PATIENT DATA ARE NOT INTENDED TO BE MEDICAL ADVICE OR INSTRUCTIONS FOR MEDICAL DIAGNOSIS, TREATMENT, OR CARE OF PERSONS BY COLLECTIVE AND THAT THE SERVICES ARE NOT A SUBSTITUTE FOR PROFESSIONAL MEDICAL ADVICE, EXAMINATION, DIAGNOSIS, OR TREATMENT AND SHOULD NOT BE USED TO DIAGNOSE, TREAT, CURE, OR PREVENT ANY DISEASE WITHOUT THE SUPERVISION OF A DOCTOR OR QUALIFIED HEALTHCARE PROVIDER. SUBSCRIBER ACKNOWLEDGES AND AGREES THAT COLLECTIVE DOES NOT OPERATE OR CONTROL THE INTERNET AND THAT: (A) VIRUSES, WORMS, TROJAN HORSES, OR OTHER UNDESIRABLE DATA OR SOFTWARE; OR (B) UNAUTHORIZED USERS (E.G., HACKERS) MAY ATTEMPT TO OBTAIN ACCESS TO AND DAMAGE DATA, WEBSITES, COMPUTERS, OR NETWORKS AND THAT COLLECTIVE WILL NOT BE RESPONSIBLE FOR SUCH ACTIVITIES EXCEPT TO THE EXTENT THAT SUCH ACTIVITIES ARE CAUSED BY COLLECTIVE'S BREACH OF ITS INFORMATION

SECURITY OBLIGATIONS HEREUNDER. IN NO EVENT SHALL COLLECTIVE BE LIABLE TO SUBSCRIBER OR ANY THIRD PARTY FOR DAMAGES CAUSED BY A ZERO-DAY SECURITY EVENT.

6. **Limitations on Liability Relating to Performance of Services.** Neither Party shall be liable to the other Party or to any third party for any incidental, consequential, or punitive damages arising out of or related to this Agreement, even if advised of the possibility of such damages. Each Party's aggregate liability to the other for all damages, losses, and causes of action, whether in contract, tort (including negligence), or otherwise shall not exceed the greater of one million dollars (\$1,000,000) or two (2) times the total fees paid to Collective on behalf of Subscriber during any twelve (12) month period of the Term. Notwithstanding the foregoing, in no event shall a Party be responsible for any penalties, damages, or other losses incurred by the other Party as the result of any event, occurrence, or failure to perform which was materially caused or contributed to by such other Party's failure to comply with an obligation under any applicable requirement of this Agreement or with any law or regulation.
7. **Indemnification.** To the extent permitted by applicable law, and subject to the limitations set forth in this Agreement, each Party will indemnify, hold harmless, and defend the other Party from and against any and all third-party claims, losses, deficiencies, damages, liabilities, costs, and other expenses (including but not limited to reasonable attorneys' fees) incurred as a result of a third-party claim which arises out of the indemnifying Party's breach of this Agreement, grossly negligent act or omission, or willful misconduct. Additionally, Collective will indemnify, hold harmless, and defend Subscriber with respect to any third-party claims, demands, awards, judgments, actions, and proceedings made by any person or organization based on a claim that the Services, without modification and without combination with any third-party's intellectual property, infringe upon a United States patent, copyright, trade secret, or other proprietary right of a third party. Notwithstanding the foregoing, Collective will have no obligation with respect to any claim of infringement that is based upon or arises out of (a) the use or combination of the Services with any software, products, data, or other materials not provided by Collective, (b) modification or alteration of the Services by anyone other than Collective, (c) use of Services in excess of the rights granted in this Agreement, or (d) any specifications, content, Patient Data or intellectual property provided by Subscriber. The indemnification obligations set forth in this Section are contingent upon the indemnified Party promptly notifying the indemnifying Party in writing of such claim, loss, liability, etc. and permitting the indemnifying Party sole authority to control the defense or settlement of such claim and providing such indemnifying Party reasonable assistance (at such indemnifying Party's sole expense) in connection therewith.
8. **Insurance.** During the Term of the Agreement, Collective shall maintain, at Collective's sole expense, commercial general liability insurance, including contractual liability and cyber liability, in the amount of \$1,000,000 per occurrence and \$5,000,000 aggregate; auto liability for \$1,000,000 combined single limit; AND workers compensation and employer's liability with limits of \$500,000 per occurrence and \$1,000,000 in aggregate. Collective shall provide proof of such insurance upon request.
9. **Term & Termination of Agreement.** The initial term of this Agreement shall be one (1) year commencing on the Effective Date (the "**Initial Term**"), after which this Agreement shall automatically renew for successive one (1) year terms (each a "**Renewal Term**" and, together with the Initial Term, the "**Term**") unless either Party provides written notice of earlier termination in accordance with this Section. This Agreement or a SOF, and Subscriber's corresponding access to the Services, may be terminated as follows:
  - 9.1. **Termination at Will.** Either Party may terminate this Agreement or a SOF at any time without cause by giving not less than ninety (90) days written notice of such termination to the other Party.
  - 9.2. **Termination for Insolvency or Bankruptcy.** Either Party may terminate this Agreement immediately upon written notice to the other Party in the event of the other Party's bankruptcy or insolvency, or the proper commencement of proceedings under bankruptcy or insolvency code or similar law, whether voluntary or involuntary, by or against such other Party, or in the event that such other Party is dissolved or liquidated.
  - 9.3. **Termination for Breach.** Except as otherwise specified in this Agreement, either Party may terminate this Agreement, effective upon written notice to the other Party, if the other Party breaches this Agreement, and such breach: (a) is incapable of a cure; or (b) being capable of cure, remains uncured thirty (30) days after the non-breaching Party provides the breaching Party with written notice of the breach (or, if the breach by its nature is not reasonably susceptible to cure within thirty (30) days, fails to commence and

diligently pursue a cure within such time period). If the breach is a failure by Subscriber to pay fees due under the applicable SOF, Collective may require a reasonable advance fee deposit or other assurance of future payments by Subscriber.

9.4. Termination for Legal Violation. This Agreement may be terminated by a non-breaching Party for cause upon breach of the other Party immediately upon written notice to the breaching Party, without any term of notice and/or judicial intervention being required, and without liability for such termination, under the following conditions:

9.4.1. *Violation of Business Associate Agreement.* Subscriber may terminate this Agreement for violation of its Business Associate Agreement by Collective, as provided in the Business Associate Agreement.

9.4.2. *Violations of Other Laws.* Either Party may terminate this Agreement upon written notice at its sole discretion in the event the other Party receives (a) a criminal conviction for any offense involving fraud, theft or malicious intent, or (b) is named as a defendant in a criminal proceeding for a violation of HIPAA.

9.5. Effect of Termination on Services. Upon termination of this Agreement for any reason, Subscriber and its Users shall no longer be authorized to use the Services, access to the Services and user names and security tokens shall be terminated, and any further access by or on behalf of Subscriber shall be prohibited unless otherwise agreed in writing by Collective.

9.6. Transition upon Termination. Upon termination of this Agreement for convenience by either Party, Collective shall, subject to Subscriber's prompt request, provide reasonable assistance to Subscriber in a transition to use of another service or system to provide services comparable to those Subscriber has subscribed to under this Agreement at the time of termination, to the extent available, provided that Collective shall require that Subscriber pay Collective's reasonable costs pertaining to such a transition.

9.7. Effect of Termination on Patient Data. Upon termination of this Agreement for any reason, Collective shall return, destroy, or if return or destruction are not feasible, retain, any Patient Data then maintained by or for Collective on behalf of Subscriber for purposes of this Agreement, under the terms of the applicable Business Associate Agreement. Subscriber acknowledges that possible reasons for which return or destruction of Patient Data may not be feasible include, but are not necessarily limited to: (a) if Patient Data has been provided to Collective and transmitted to other subscribers for purposes of Collective carrying out its obligations to provide services for which Subscriber has contracted, or (b) if Patient Data has become part of a record owned or maintained by or for another subscriber and is therefore subject to that subscriber's ownership and corresponding business associate agreement governing Collective's treatment and care of such data.

## 10. Mutual Confidentiality.

10.1. Definition. For purposes of this Agreement, "**Confidential Information**" means any non-public information of either Party relating to its business activities, financial affairs, technology, marketing or sales plans that is disclosed to, and received by, whether orally or in writing, the other Party pursuant to this Agreement, including any information that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure, and the terms and conditions of this Agreement and any associated SOF. Subscriber acknowledges and agrees that the technology and computer code underlying the Services is Confidential Information of Collective.

10.2. Protection. Each Party agrees (a) to exercise the same degree of care and protection with respect to the other Party's Confidential Information as each Party exercises with respect to its own similar information, but in no event less than a reasonable degree of care and protection; and (b) not to disclose such Confidential Information to any third party or use it for any purposes other than in connection with fulfilling its obligations under, or enjoying the rights granted to it, under this Agreement; provided, however, that each Party may disclose Confidential Information to its employees and third parties performing services for such Party related to the purposes of this Agreement who have a need to know such Confidential Information and who have agreed in writing to comply with the restrictions set forth herein with respect to such Confidential Information.

10.3. Exceptions. If Subscriber is a government entity, then the obligations set forth in this Section 10 shall apply only to the extent legally permissible. Furthermore, These obligations shall not apply to Confidential

Information which (a) is known by the receiving Party prior to its receipt, as evidenced by written documentation, (b) is now or hereafter becomes publicly known by acts not attributable to the receiving Party, (c) is disclosed to a Party by a third party who has the legal right to make such disclosure, (d) is disclosed by a Party with the other Party's separate written consent, or (e) is required to be disclosed pursuant to governmental regulation or court order.

## 11. Miscellaneous.

- 11.1. Access to Records. If required for purposes of 42 CFR §420.300, or any other applicable state or federal law, upon written request Collective shall make any necessary books, records, and documents available to the U.S. Department of Health and Human Services Comptroller General, their duly authorized representatives, or other governmental authority, for purposes of verifying the nature and extent of any costs incurred by Subscriber for services furnished by Collective for which payment may be or have been made under Medicare, Medicaid, or other applicable federal or state reimbursement programs. Collective's obligation to provide access to records under this Section shall survive the termination of this Agreement for such periods required by applicable law.
- 11.2. OIG Exclusions. Collective will screen all of its current and prospective owners, legal entities, officers, directors, employees, contractors, and agents ("**Screened Persons**") against (a) the United States Department of Health and Human Services Office of Inspector General's List of Excluded Individuals/Entities (LEIE), or (b) the System for Awards Management to ensure that none of the Screened Persons are currently excluded, debarred, suspended, or otherwise ineligible to participate in Federal healthcare programs or in Federal procurement or nonprocurement programs, (each, an "**Ineligible Person**"). If at any time during the Term any Screened Person becomes an Ineligible Person or is proposed to be an Ineligible Person, Collective shall promptly cease permitting such Ineligible Person to perform services hereunder.
- 11.3. Force Majeure. No Party will be liable for any failure to perform its obligations hereunder where such failure results from force majeure, meaning any cause beyond the reasonable control of the Party and which could not have been prevented through the exercise of reasonable care and precautions, including acts of god, fire, strike, lockout, labor disputes, accidents, war, civil insurrection, riots, embargoes, or the demands, restrictions, or delays of any government.
- 11.4. Applicable Law. This Agreement shall be interpreted consistently with applicable federal law and with the state laws of Subscriber's state of domicile, without regard to such state's choice-of-law principles.
- 11.5. Dispute Resolution. In the event of any dispute between the Parties arising out of this Agreement, the Parties shall use their best efforts to resolve the dispute through face-to-face, good faith negotiations. Disputes not resolved within sixty (60) days following notice of the dispute shall be submitted to binding arbitration by a single arbitrator selected by both Parties, and judgment upon the award rendered by the arbitrator may be entered in any court having jurisdiction over the Parties. The arbitrator may award the prevailing Party the costs and reasonable attorneys' fees expended in such arbitration.
- 11.6. Amendment. As a condition to Subscriber's participation in the Collective Network, Collective reserves the right to modify the terms of this Agreement (including the Network Policies) for any reason related to legal, regulatory, technical, or operational necessities, following one hundred twenty (120) days notice to Subscriber thereof. The Parties may otherwise amend this Agreement by a written instrument executed by both Parties.
- 11.7. Assignment. Neither Party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the other Party's prior written consent (not to be unreasonably withheld); provided, however, that either Party may assign this Agreement in its entirety (including all SOFs), without the other Party's consent to its Affiliate or to its legal successor in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets. Notwithstanding the foregoing, if a Party is acquired by, sells substantially all of its assets to, or undergoes a change of control in favor of, a direct competitor of the other Party, such other Party may terminate this Agreement upon written notice. In the event of such a termination, Collective shall refund Subscriber any subscription fees which were prepaid by Subscriber for such cancelled portion of the Term. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the Parties, their respective successors, and permitted assigns.

- 11.8. Notices. The Parties hereby consent to the giving and receipt of notices as follows, and such notices shall be deemed to be effectively given upon receipt of the receiving Party if (a) hand delivered, (b) sent postage prepaid via certified mail, return receipt requested, (c) mailed for overnight delivery, or (d) delivered via email, provided that, in each case, the sending Party utilizes the notice address(es) indicated on the signature page hereto. Furthermore, in the case of a notice via email, the sending Party shall ensure that the transmission of such notice is time-stamped and that the original notice document is reasonably protected against alteration. Each Party may change its address(es) for notices by the providing notice thereof to the other Party in accordance with this Section.
- 11.9. Severability. If any portion of this Agreement is declared void or ineffective by a court of competent jurisdiction, such portions shall be ineffective only to the extent of such invalidity or unenforceability, and the remaining portions shall remain valid, enforceable, and in full effect.
- 11.10. No Waiver. No failure or delay on the part of either Party in exercising any right, power, or remedy under this Agreement will operate as a waiver thereof, nor will any single or partial exercise of any such right, power, or remedy preclude any other or further exercise thereof or the exercise of any other right, power, or remedy hereunder. The rights and remedies provided in this Agreement are cumulative, and are not exclusive of any other rights, powers, or remedies, now or hereafter existing, at law or in equity or otherwise.
- 11.11. Third Party Beneficiaries. Except as may be expressly set forth in an addendum or attachment hereto, neither this Agreement nor any attachment hereto is intended for the benefit of any third party, and no third party shall have any cause of action arising from or pertaining to it.
- 11.12. Survival. Sections 1, 2.5, 5, 6, 7, **Error! Reference source not found.**, 9.5, 9.6, 9.7, 10, and 11 shall survive the termination of this Agreement for any reason. Certain sections of the Network Policies and BAA may also survive the termination of this Agreement, as set forth therein.
- 11.13. Counterparts; Facsimiles. This Agreement may be executed and retained in counterparts, each of which will constitute an original and all of which will be one and the same document. Facsimile copies shall be deemed to be originals. The Parties hereby consent to the use of electronic contracting. Any document related hereto which may require a signature may be signed by an electronic signature using Adobe, DocuSign, or a similar software application.
- 11.14. Entire Agreement; Interpretation. Except where expressly stated otherwise, references to this Agreement shall be interpreted as referring to the main body of this Master Subscription Agreement as well as to the Network Policies and to all other schedules, exhibits, attachments, SOWs, addendums, and amendments hereto, including, without limitation, the BAA. This Agreement constitutes the sole and entire agreement of the Parties with respect to the subject matter hereof and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, with respect to the subject matter hereof. In the event of any inconsistency or ambiguity between any of the provisions of this Agreement, it shall be resolved according to the following order of priority: (i) the BAA, (ii) the SOF(s), with respect to each individual SOF only, (iii) the main body of this Master Subscription Agreement, (iv) the Network Policies, and (v) all other documents incorporated herein by reference.

\*\*\* Signature Page Follows \*\*\*

**IN WITNESS WHEREOF**, Collective and Subscriber have executed this Master Subscription Agreement as of the Effective Date.

**COLLECTIVE MEDICAL TECHNOLOGIES, INC.**

**NAPA COUNTY HEALTH AND HUMAN SERVICES AGENCY**

By: Christopher Alworth \_\_\_\_\_

By: \_\_\_\_\_

Chris Alworth  
Printed Name

BELIA RAMOS  
Printed Name

Associate General Counsel, Acute & Payer  
Title

Chair of the Board of Supervisors  
Title

| Collective Address for Notices  | Subscriber Address for Notices   |
|---|--|
| Attn: Legal<br>4760 S. Highland Drive #217<br>Holladay, UT 84117<br><br>Fax: (855) 343-7671<br>Email: legal@collectivemedicaltech.com | <u>2751 Napa Valley Corporate Dr., Bldg. A</u><br>Address 1<br><u>Mental Health Services Division</u><br>Address 2<br><u>Napa, California 94503</u><br>Address 3<br><br>_____<br>Fax<br><br>_____<br>Email |
|   | Subscriber Contact for Invoices  |
|   | _____<br>Name<br><br>_____<br>Email<br><br>_____<br>Phone  |

|  |   |  |
|--|---|--|
| APPROVED AS TO FORM<br>Office of County Counsel<br>By: <u>Rachel L. Ross (e-signature)</u><br>Deputy County Counsel<br><br>Date: 10/5/2022 | APPROVED BY THE NAPA COUNTY<br>BOARD OF SUPERVISORS<br><br>Date: _____<br>Processed By:<br><br>_____<br>Deputy Clerk of the Board | ATTEST: NEHA HOSKINS<br>Clerk of the Board of Supervisors<br><br>By: _____ |
|--|---|--|

## Master Subscription Agreement Attachment A: Service Level Agreement

### 1. Availability:

“**Availability**” means the percentage of time each month, exclusive of scheduled maintenance, that the Services web portal (the “**Application**”) shall be available to Subscriber on a continuous basis, 24 hours per day, 7 days per week, 365 days per year. Collective commits that the Application will be provided at a monthly Availability of 99.9% or greater.

### 2. Non-Performance Penalties:

In the event that the Availability percentage falls below the top committed range shown in the table below, Subscriber’s subsequent invoice for Services will be credited in an amount equal to the indicated percentage of Subscription Fees prorated for the month of such failure.

| Committed Range         |                                      |
|-------------------------|--------------------------------------|
| Availability Percentage |                                      |
| <b>100% to 99.9%</b>    | Service Fees Due As Invoiced         |
| Below Committed Range   |                                      |
| Availability Percentage | Percentage of Monthly Invoice Credit |
| 99.89% - 99.0%          | 5%                                   |
| 98.99% - 98%            | 10%                                  |
| 97.99% - 90%            | 20%                                  |
| Below 90%               | 30%                                  |

### 3. Non-Performance Remedies:

If Collective fails to provide the Application on a continuous basis for at least ninety-five percent (95%) of the time for three (3) consecutive calendar months, Subscriber may terminate the Agreement, regardless of any term remaining, without liability for penalties or damages associated with such termination, upon five (5) days prior written notice. In such event Collective shall refund any prepaid fees for periods after termination.

### 4. Non-Performance Reporting:

Upon request by Subscriber, Collective shall provide a report showing Availability based on the foregoing requirements and setting forth the credits, if any, due to Subscriber as provided above. Any credits issued under this Service Level Agreement are cumulative and shall be in addition to any other rights or remedies Subscriber may have under the Agreement or at law or in equity.

### 5. Technical Support

#### a. Escalation Definitions:

Collective shall acknowledge and correct any Technical Errors (defined below) in the applicable Application reported by Subscriber or otherwise known to Collective in accordance with the priority levels reasonably assigned by Subscriber to such error, as set forth in this Section 5. A “**Technical Error**” may be defined as one of the following:

- “**Severity 1 Error**” means an error that renders the Application inoperative or unavailable or causes a data privacy or security issue.
- “**Severity 2 Error**” means an error that causes a serious work stoppage or makes it impossible for Subscriber or any Users of the Application to accomplish a critical business task.
- “**Severity 3 Error**” means an error that is disrupting work or causing delays or annoyance, but there are workarounds that enable Subscriber or its Users to complete critical business tasks.

| <b>Error</b>     | <b>Response Time/Communications</b>  | <b>Supplier Action to Resolve</b>  |
|------------------|--|--|
| Severity Level 1 | 1 hour - Acknowledgment of receipt of error report and identification of individual assigned to resolve error.   | Immediately and continuously work (24 x 7 x 365) until error correction achieved. Escalate if not corrected within 24 hours.<br><br>If a workaround is provided for a Severity Level 1 Error, Collective will use continuous work efforts (24 x 7 x 365) to correct the Severity 1 Error unless otherwise agreed by Subscriber in writing. |
| Severity Level 2 | 6 hours - Acknowledgment of receipt of error report and identification of individual assigned to resolve error.  | Immediately create “Hot Fix” priority software development ticket and provide acceptable workaround or error correction as soon as reasonably possible. If acceptable workaround provided, the Hot Fix Ticket will be re-classified as a Bug Fix Ticket under Severity Level 3 below.  |
| Severity Level 3 | 48 hours - Acknowledgment of receipt of error report and identification of individual assigned to resolve error. | Create “Bug Fix Ticket” to be prioritized as a software development item as time and resources allow.  |

**b. Technical Support Reporting Procedures:**

Subscriber shall report Severity Level 1 or Level 2 Technical Errors via telephone at (509) 590-4443 and Severity Level 3 Technical Errors via email at [support@collectivemedicaltech.com](mailto:support@collectivemedicaltech.com).

**c. Support Failure Remedies:**

If, in any given calendar month, Collective fails to respond to errors in accordance with the service levels set forth above, Subscriber shall receive a credit on its subsequent applicable Subscription Fee invoice as set forth below.

| <b>Response Time Failures</b>   | <b>Percentage Credit</b> |
|---|--------------------------|
| Severity 1 Errors -- failure to respond in timely fashion two or more times | 10%                      |
| Severity 2 Errors -- failure to respond in timely fashion two or more times | 5%                       |
| Severity 3 Errors -- failure to respond in timely fashion two or more times | 2%                       |

## **Master Subscription Agreement Attachment B: HIPAA Business Associate Agreement**

This Exhibit shall constitute the Business Associate Agreement (the “Agreement”) between **Collective Medical Technologies, Inc.**, (the “Business Associate”) and Napa County (the “Covered Entity”), and applies to the functions Business Associate will perform on behalf of Covered Entity (collectively, “Services”), that are identified in the Master Agreement (as defined below).

1. **Purpose.** This Agreement is intended to ensure that the Business Associate will establish and implement appropriate privacy and security safeguards with respect to “Protected Health Information” (as defined below) that the Business Associate may create, receive, maintain, transmit, use, or disclose in connection with the Services to be provided by the Business Associate to the Covered Entity, and that such safeguards will be consistent with the standards set forth in regulations promulgated under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”) as amended by the Health Information Technology for Economic and Clinical Health Act as set forth in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (“HITECH Act”).

2. **Regulatory References.** All references to regulatory Sections, Parts and Subparts in this Agreement are to Title 45 of the Code of Federal Regulations as in effect or as amended, and for which compliance is required, unless otherwise specified.

3. **Definitions.** Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms are defined in Sections 160.103, 164.304 and 164.501.

(a) **Business Associate.** “Business Associate” shall mean the party identified above as the “Business Associate”.

(b) **Breach.** “Breach” shall have the same meaning as the term “breach” in Section 164.402.

(c) **Covered Entity.** “Covered Entity” shall mean the County of Napa, a hybrid entity, and its designated covered components, which are subject to the HIPAA Rules.

(d) **Designated Record Set.** “Designated Record Set” shall have the same meaning as the term “designated record set” in Section 164.501.

(e) **Electronic Media.** “Electronic Media” shall have the same meaning as the term is defined in Section 160.103.

(f) **Electronic Protected Health Information.** “Electronic Protected Health Information” (“EPHI”) is a subset of Protected Health Information and means individually identifiable health information that is transmitted or maintained in electronic media, limited to the information created, received, maintained or transmitted by Business Associate from or on behalf of Covered Entity.

(g) **HIPAA Rules.** “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

(h) **Individual.** “Individual” shall have the same meaning as the term “Individual” in Section 164.501 and shall include a person who qualifies as a personal representative in accordance with Section 164.502(g).

(i) **Master Agreement.** “Master Agreement” shall mean the Master Subscription Agreement to which this Exhibit is attached and made a part of.

(j) **Minimum Necessary.** “Minimum Necessary” shall mean the minimum amount of Protected Health Information necessary for the intended purpose, as set forth at Sections 164.502(b) & 164.514(d): *Standard: Minimum Necessary.*

(k) Privacy Rule. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at Part 160 and Part 164, Subparts A and E.

(l) Protected Health Information. “Protected Health Information” shall have the same meaning as the term “protected health information” in Section 160.103, limited to the information received from Covered Entity or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

(m) Required By Law. “Required by law” shall have the same meaning as the term “required by law” in Section 164.103.

(n) Secretary. “Secretary” shall mean the Secretary of the United States Department of Health and Human Services (“DHHS”) or his/her designee.

(o) Security Incident. “Security Incident” shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of personally identifiable information. A Security Incident includes the attempted or successful unauthorized access, use, disclosure, modification, or destruction of or interference with systems operations in an information system which processes Protected Health Information that is under the control of Covered Entity, or Business Associate of Covered Entity, but does not include minor incidents that occur on a daily basis, such as scans, “pings”, or unsuccessful random attempts to penetrate computer networks or servers maintained by Business Associate.

(p) Security Rule. “Security Rule” shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.

(q) Subcontractor. “Subcontractor” means a subcontractor of Business Associate that creates, receives, maintains, or transmits Protected Health Information on behalf of the Business Associate.

(r) Unsecured Protected Health Information. “Unsecured Protected Health Information” shall have the same meaning as the term “unsecured protected health information” in Section 164.402, limited to the information received from Covered Entity or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

#### 4. **Business Associate’s Obligations and Compliance with the HIPAA Privacy and Security Rules.**

(a) Business Associate acknowledges that it is directly required to comply with the HIPAA Rules and that Business Associate (including its subcontractors) may be held directly liable and subject to penalties for failure to comply. To the extent the Business Associate is to carry out one or more of Covered Entity’s obligations under Subpart E of 45 CFR Part 164 of the Privacy Rule, Business Associate agrees to comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligations.

(b) Business Associate agrees not to use or further disclose Protected Health Information other than as permitted or required by this Agreement, or as required by law.

(c) Business Associate shall not sell Protected Health Information.

#### 5. **Permitted Uses and Disclosures.**

(a) Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity for the purposes specified in the Master Agreement, subject to limiting use and disclosure to applicable minimum necessary rules, regulations and statutes and provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity. Business Associate must make reasonable efforts to limit Protected Health Information to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request.

(b) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(c) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are

Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(d) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by Section 164.504(e)(2)(i)(B).

(e) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities consistent with Section 164.502(j).

(f) Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 of the Privacy Rule if done by Covered Entity, except for the specific uses and disclosures set forth herein.

## 6. **Appropriate Safeguards.**

(a) Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of Protected Health Information other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Protected Health Information that is created, received, maintained or transmitted on behalf of the Covered Entity and limiting use and disclosure to the Minimum Necessary.

(b) Safeguarding Electronic Protected Health Information. Business Associate agrees to comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information. Business Associate must secure all Electronic Protected Health Information by technological means that render such information unusable, unreadable, or indecipherable to unauthorized individuals and in accordance with the National Institute of Standards Technology (NIST) Standards and Federal Information Processing Standards (FIPS) as applicable, Should Business Associate fail to comply with this provision, it agrees to hold harmless, defend at its own expense and indemnify Covered Entity in accordance with the terms of Section 9 of the Agreement, "Indemnification".

(c) Destruction of Protected Health Information on paper, film, or other hard copy media must involve either shredding or otherwise destroying the Protected Health Information so that it cannot be read or reconstructed.

(d) Should any employee or subcontractor of Business Associate have direct, authorized access to computer systems of Covered Entity that contain Protected Health Information, Business Associate shall immediately notify Covered Entity of any change of such personnel (e.g. employee or subcontractor termination, or change in assignment where such access is no longer necessary) in order for Covered Entity to disable the previously authorized access.

## 7. **Reporting Unauthorized Uses and Disclosures.**

(a) Business Associate agrees to notify Covered Entity of any access, use or disclosure of Protected Health Information not permitted or provided for by the Agreement of which it becomes aware, including any breach as required at Section 164.410, or security incident. Such notification will be made immediately after discovery by telephone call at 707.253.4715, plus e-mail at Privacy.Officer@countyofnapa.org, and will include, to the extent possible, the identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used or disclosed, a description of the Protected Health Information involved, the nature of the unauthorized access, use or disclosure, the date of occurrence, and a description of any remedial action taken or proposed to be taken by Business Associate. Business Associate will also provide to Covered Entity any other available information that the Covered Entity is required to include in its notification to the Individual under Section 164.404(c) at the time of the initial report or promptly thereafter as the information becomes available.

(b) In the event of a request by law enforcement under Section 164.412, Business Associate may delay notifying Covered Entity for the applicable timeframe.

(c) A breach or unauthorized access, use, or disclosure shall be treated as discovered by the Business Associate on the first day on which such unauthorized access, use, or disclosure is known, or should reasonably have

been known, to the Business Associate or to any person, other than the individual committing the unauthorized disclosure, that is an employee, officer, subcontractor, agent or other representative of the Business Associate.

(d) In meeting its obligations under this section, it is understood that Business Associate is not acting as the Covered Entity's agent. In performance of the work, duties, and obligations and in the exercise of the rights granted under this Agreement, it is understood and agreed that Business Associate is at all times acting as an independent contractor in providing services pursuant to this Agreement and the Master Agreement.

**8. Mitigating the Effect of a Breach, Security Incident, or Unauthorized Access, Use or Disclosure of Unsecured Protected Health Information.**

(a) Business Associate agrees to mitigate, to the greatest extent possible, any harm that results from the breach, security incident, or unauthorized access, use or disclosure of Unsecured Protected Health Information by Business Associate or its employees, officers, subcontractors, agents, or other representatives.

(b) Following a breach, security incident, or any unauthorized access, use or disclosure of Unsecured Protected Health Information, Business Associate agrees to take any and all corrective action necessary to prevent recurrence, to document any such action, and to make this documentation available to Covered Entity.

(c) Except as required by law, Business Associate agrees that it will not inform any third party of a breach or unauthorized access, use or disclosure of Unsecured Protected Health Information without obtaining the Covered Entity's prior written consent. Covered Entity hereby reserves the sole right to determine whether and how such notice is to be provided to any Individuals, regulatory agencies, or others as may be required by law, regulation or contract terms, as well as the contents of such notice. When applicable law requires the breach be reported to a federal or state agency or that notice be given to media outlets, Business Associate shall cooperate with and coordinate with Covered Entity to ensure such reporting is in compliance with applicable law and to prevent duplicate reporting, and to determine responsibilities for reporting.

**9. Indemnification.**

(a) Subject to the limitations set forth in the Master Agreement, Business Associate agrees to hold harmless, defend at its own expense, and indemnify Covered Entity for the costs of any mitigation undertaken by Business Associate pursuant to Section 8, above.

(b) Business Associate agrees to assume responsibility for any and all costs associated with the Covered Entity's notification of Individuals affected by a breach or unauthorized access, use or disclosure by Business Associate or its employees, officers, subcontractors, agents or other representatives when such notification is required by any state or federal law or regulation, or under any applicable contract to which Covered Entity is a party.

(c) Subject to the limitations set forth in the Master Agreement, Business Associate agrees to hold harmless, defend at its own expense and indemnify Covered Entity, including Covered Entity's employees, directors, officers, subcontractors, agents or other members of its workforce (each of the foregoing hereinafter referred to as "Indemnified Party"), against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with any breach of this Agreement or from any acts or omissions related to this Agreement by Business Associate or its employees, directors, officers, subcontractors, agents or other members of its workforce. Accordingly, Business Associate shall reimburse any Indemnified Party for any and all actual and direct losses, liabilities, lost profits, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third party which results from the Business Associate's acts or omissions hereunder. Business Associate's obligation to indemnify any Indemnified Party shall survive the expiration or termination of this Agreement.

(d) Survival. The obligations of Business Associate under this Section 9 shall survive this Agreement.

**10. Individuals' Rights.**

(a) Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner designated by the Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under Section 164.524.

(b) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to make pursuant to Section 164.526, at the request of Covered Entity or an Individual, and in the time and manner designated by the Covered Entity.

(c) Business Associate agrees to document such disclosures of Protected Health Information 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 Protected Health Information in accordance with Section 164.528.

(d) Business Associate agrees to provide to Covered Entity or an Individual, in the time and manner designated by Covered Entity, information collected in accordance with Section 10(c) of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with Section 164.528.

(e) Business Associate agrees to comply with any restriction to the use or disclosure of Protected Health Information that Covered Entity agrees to in accordance with Section 164.522.

**11. Obligations of Covered Entity.**

(a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with Section 164.520, as well as any changes to such notice.

(b) Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with Section 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

**12. Agents and Subcontractors of Business Associate.**

(a) Business Associate agrees to enter into written agreements with any agent, subcontractor or vendor, to whom it provides Protected Health Information received from Covered Entity or created, received, maintained or transmitted by Business Associate on behalf of Covered Entity, that impose the same restrictions, conditions and requirements that apply through this Agreement to Business Associate with respect to such information, including the requirement to immediately notify the Business Associate of any instances of any breach, security incident, intrusion, or unauthorized access to or use or disclosure of Protected Health Information of which it becomes aware. Upon request, Business Associate shall provide copies of such agreements to Covered Entity.

(b) Business Associate shall implement and maintain sanctions against any agent, subcontractor or other representative that violates such restrictions, conditions or requirements and shall mitigate the effects of any such violation.

**13. Audit, Inspection, and Enforcement.**

(a) Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from Covered Entity or created, received, maintained, or

transmitted by Business Associate on behalf of Covered Entity, available to any state or federal agency, including the Secretary, for the purposes of determining compliance with HIPAA and any related regulations or official guidance.

(b) Business Associate will undergo annual certification with the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF), or other reasonable certification alternative such as Service Organization Controls 2 (SOC 2) Type II based on Trust Services Principles and designed to evaluate and report compliance with HIPAA and other applicable federal and state laws (each an "Assessment"). Assessments will be conducted at Business Associate's operations center at Business Associate's cost by an independent assessor. Summaries of all reports related to the Assessments be provided to Covered Entity upon request.

14. **Permissible Requests by Covered Entity.** Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

15. **Term and Termination.**

(a) The terms of this Agreement shall remain in effect for the duration of all services provided by Business Associate under the Master Agreement and for so long as Business Associate remains in possession of any Protected Health Information received from Covered Entity, or created, received, maintained or transmitted by Business Associate on behalf of Covered Entity unless Covered Entity has agreed in accordance with this Section 15 that it is not feasible to return or destroy all Protected Health Information.

(b) Upon termination of the Master Agreement, Business Associate shall recover any Protected Health Information relating to the Master Agreement and this Agreement in its possession and in the possession of its subcontractors, agents or representatives. Business Associate shall return to Covered Entity, or destroy with the consent of Covered Entity, all such Protected Health Information, in any form, in its possession and shall retain no copies.

(c) If Business Associate believes it is not feasible to return or destroy the Protected Health Information, Business Associate shall so notify Covered Entity in writing. The notification shall include: (1) a statement that the Business Associate has determined that it is not feasible to return or destroy the Protected Health Information in its possession, and (2) the specific reasons for such determination. Business Associate may retain only that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities. If Covered Entity agrees in its sole discretion that Business Associate cannot feasibly return or destroy the Protected Health Information, Business Associate shall ensure that any and all protections, requirements and restrictions contained in the Master Agreement and this Agreement shall be extended to any Protected Health Information for so long as Business Associate maintains such Protected Health Information, and that any further uses and/or disclosures will be limited to the purposes that make the return or destruction of the Protected Health Information infeasible.

(d) Covered entity may immediately terminate the Master Agreement if it determines that Business Associate has violated a material term of this Agreement.

(e) Survival. The obligations of Business Associate under this Section 15 shall survive this Agreement.

16. **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity and Business Associate to comply with the requirements of the HIPAA Rules.

17. **Entire Agreement.** This Exhibit constitutes the entire HIPAA Business Associate Agreement between the parties, and supersedes any and all prior HIPAA Business Associate Agreements between them.

18. **Notices.**

(a) All notices required or authorized by this Agreement shall be in writing and shall be delivered in person or by deposit in the United States mail, by certified mail, postage prepaid, return receipt requested. Any notice sent by mail in the manner prescribed by this paragraph shall be deemed to have been received on the date noted on the return receipt or five days following the date of deposit, whichever is earlier.

(b) Any mailed notice, demand, request, consent, approval or communication that Covered Entity desires to give to Business Associate shall be addressed to Business Associate at the mailing address set forth in the Master Agreement.

(c) Any mailed notice, demand, request, consent, approval or communication that Business Associate desires to give to Covered Entity shall be addressed to Covered Entity at the following address:

Napa County Compliance and Privacy Officer  
2751 Napa Valley Corporate Dr. Suite B  
Napa, CA 94559  
707.253.4715

(d) For purposes of subparagraphs (b) and (c) above, either party may change its address by notifying the other party of the change of address.

**19. Lost Revenues; Penalties/Fines.**

(a) Penalties/Fines for Failure to Comply with HIPAA. Subject to the limitations set forth in the Master Agreement, Business Associate shall pay any penalty or fine assessed against Covered Entity arising from Business Associate's failure to comply with the obligations imposed by HIPAA.

(c) Penalties/Fines (other). Subject to the limitations set forth in the Master Agreement, Business Associate shall pay any penalty or fine assessed against Covered Entity arising from Business Associate's failure to comply with all applicable Federal or State Health Care Program Requirements, including, but not limited to any penalties or fines which may be assessed under a Federal or State False Claims Act provision.