



PHASE I PILOT PARTICIPATION AGREEMENT

To confirm this Agreement, please sign and return a copy of this Agreement. A fully executed copy will be returned to you for your files. This Agreement is subject to the terms and conditions set forth on the following pages. By signing below, Participant has read and understands the terms and conditions of this Agreement.

Accepted by:

AUTHORIZED SIGNATORY PARTICIPANT: [Insert Name] [ADDRESS Line 1] [ADDRESS Line 2]	AUTHORIZED SIGNATORY VCCIE, a program of Public Health Institute: Public Health Institute 1950 Franklin Street, Suite 600 Oakland, CA 94612
(Signature)	(Signature)
(Date)	(Date)
Name: [Insert Name]	Rebecca Silva
Title: [Insert Title]	Vice President of Program Award Management



PHASE I PILOT PARTICIPATION AGREEMENT

VCCIE Phase I Pilot Participation Agreement

This VCCIE Phase I Pilot Participation Agreement (“Agreement”) is entered into between Public Health Institute, on behalf of its program Ventura County Community Information Exchange (“VCCIE”), with its principal place of operation located at 1950 Franklin Street, Suite 600, Oakland, CA 94612, and [insert name] with its principal place of business located at [insert address] (“the Participant”), each a “Party” and collectively, the “Parties” do enter into this Agreement upon the terms and conditions provided herein.

RECITALS:

WHEREAS, the information exchange architecture discussed herein consists of a technology platform that will be piloted by health care providers and community institution members, including the Participant (such health care providers and community institution members and the Participant hereinafter referred to collectively as “Participants” or individually as “a Participant”) that agree to use the Ventura County Community Information Exchange Database (“Database”) to exchange information necessary for support of Client referrals and services as offered and/or otherwise provided by Participants. The role for the VCCIE includes providing or arranging for the provision of information transmission and related services through the Database, including direct referral services and in some cases closed loop referral services, to allow Participants to conduct searches for members of the Ventura County public (“Clients”) and their related data, and to exchange such data identified from those searches through a web-based portal that facilitates the sharing of Client Data (as defined below) among disparate Participants. The Database will also maintain a directory of participating professionals, agencies, and businesses that provide services associated with social determinants of health, doing so in support of making eligible connections for Clients with community resources enabling access to medical care, mental health services, housing, food, clothing, government benefits, and other services as may be identified.

WHEREAS, the VCCIE will maintain the Database such that the Database may serve as a source of information, for Participants about a Client’s current needs and eligibility to access community resources suitable to address those needs. VCCIE’s services include establishing and applying standards for such exchange of information. VCCIE has access to and/or is responsible to ensure the maintenance of some or all of such information in the performance of VCCIE’s services. VCCIE also aggregates and/or maintains a repository of Client Data.

PHASE I PILOT PARTICIPATION AGREEMENT

WHEREAS, the information maintained in the Database consists of information provided by the Client (“self-reported”) and information entered into the Database by Participants, for which a Participant has an appropriate Authorization to allow such information to be entered into and accessible through the Database by Participants and VCCIE (collectively, any and all information entered into the Database or otherwise in the possession and/or control of the VCCIE that is provided or created under a valid Client Authorization is hereinafter referred to as “Client Data”).

WHEREAS, the Parties must, prior to processing any Client Data hereunder, agree to the terms of a Business Associate Addendum (“BAA”), attached here as Exhibit A, pursuant to the HIPAA Rules wherein the Parties agree to observe and faithfully perform the duties and obligations of a Business Associate, and Covered Entity, as the context may require.

THEREFORE, in consideration of the Parties’ obligations hereunder and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the following provisions of this Agreement.

1.0 DEFINITIONS.

- 1.1 Capitalized Terms** used in this Agreement but not defined immediately below are defined where they are used with the meanings indicated herein. Those terms, acronyms, and phrases utilized in the information technology or health and social determinants of health support services fields that are not otherwise defined in this Agreement or the BAA (as applicable), including any attachments to the same, will be interpreted per their generally understood meaning in such industry or business context.
- 1.2 Rules of Interpretation.** If, and to the extent there is a conflict between the definition given a term by this Agreement and the BAA or other attachment, the definition stated in the BAA shall govern, otherwise the definition given in this Agreement shall govern. The following terms are defined by HIPAA and incorporated herein as if fully restated: “Business Associate Agreement,” “Breach,” “Permitted Use” “Protected Health Information” and “Security Incident.”
- 1.3 Defined Terms.**
- 1.3.1 “Agreement”** means this VCCIE PHASE I PILOT PARTICIPATION AGREEMENT, as well as all schedules, exhibits, and appendices that, upon execution, are incorporated by reference herein, as may be executed or amended from time to time by the Parties in accordance with terms and conditions of this Agreement.
- 1.3.2 “Applicable Law”** means all laws which govern the subject matter



PHASE I PILOT PARTICIPATION AGREEMENT

of this Agreement, including without limitation all federal, state and local laws which govern the privacy and security of personally identifiable and sensitive information under State Law and protected health information under both State and Federal Laws and Regulations. Applicable Laws include without limitation FERPA, PPRA, HIPAA, HITECH, Confidentiality of Substance Use Disorder Patient Records at 42 C.F.R. Part 2 et seq., CMIA, the Pupil Records Act at California Education Code Sections 49060 et seq., California Civil Code Sections 56.05, 56.10, 56.11, 1798.24, and 1798.80 et seq, and California Welfare and Institutions Code Sections 5328 et seq.

- 1.3.3 **“Authorized User”** means an individual Participant or an individual designated by a Participant to access and use the Database, including without limitation, an employee or Business Associate of the Participant.
- 1.3.4 **“Authorization”** means and refers to a written authorization satisfying the requirements of 45 CFR Section 164.508, 42 CFR Part 2, and/or California Civil Code Section 56.11, or other Applicable Law that requires a patient’s express written permission for the disclosure of health information including certain types of sensitive healthcare information such as drug or alcohol abuse information by a federal or state program, or HIV Test Results; or that requires a student’s, or their representative’s, express written permission for the disclosure of education or student records.
- 1.3.5 **“Client”** means an individual receiving health care, mental health, or social services or government benefits from a Participant or referral services from the VCCIE whose information will be shared pursuant to this Agreement with other Participants. Client does not mean or include those clients whose information is not entered into the Database.
- 1.3.6 **“Client Authorization”** means and refers to a Client’s express permission for a Participant to use or disclose the Client’s Data to the VCCIE and other Participants. VCCIE’s preferred Client Authorization Form is attached here as Exhibit B.
- 1.3.7 **“Client Data”** means the information relating to a Client, including without limitation, personally identifiable information and protected health information; name, address, telephone number, financial information, health condition and other information relevant to the provision of services.

PHASE I PILOT PARTICIPATION AGREEMENT

- 1.3.8 **“CMIA”** means the California Confidentiality of Medical Information Act, California Civil Code Section 56 et. seq.
- 1.3.9 **“Community”** means the VCCIE and all Participants registered to use the Database, collectively.
- 1.3.10 **“Consent”** means a Client’s express acknowledgement of Client’s agreement, and all consents necessary to memorialize such agreement, to be involved as a Client in the Community Information Exchange, and Consent as used herein includes the Client Authorization.
- 1.3.11 **“Database”** means the software and hardware systems owned and operated by or on behalf of the VCCIE and the processes and procedures, collectively, that enables access, retrieval, use, disclosure and exchange of Participant and Client Data between the VCCIE and the Participants through the Database.
- 1.3.12 **“Educational Institution (EI) Participant”** means a Participant that is an institution of learning that is subject to FERPA and/or PPRA.
- 1.3.13 **“FERPA”** means the Family Educational Rights and Privacy Act and its implementing regulations promulgated thereunder at 34 C.F.R. Part 99, as amended.
- 1.3.14 **“HIPAA”** means the Health Insurance Portability and Accountability Act of 1996, as amended by HITECH, and its implementing regulations promulgated thereunder at 45 C.F.R. Parts 160 and 164.
- 1.3.15 **“HIPAA Privacy Rule”** means the federal regulations at 45 C.F.R. Part 160 and Subparts A and E of Part 164.
- 1.3.16 **“HIPAA Security Rule”** means the federal regulations at 45 C.F.R. Part 160 and Subpart C of Part 164.
- 1.3.17 **“HITECH”** means the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (commonly known as “ARRA”), Pub. L. No. 111-5 (February 17, 2009).
- 1.3.18 **“Participant”** means an individual or entity that has entered into a Participation Agreement with the VCCIE. References to Participant include its employees, agents, contractors, and Authorized Users if and to the extent such individual accesses the Database or Client Data.
- 1.3.19 **“Permission”** means a valid Authorization or authority granted by Applicable Law to allow for the exchange or use of Client Data.

PHASE I PILOT PARTICIPATION AGREEMENT

- 1.3.20 “Permitted Use(s)”** means all activities in connection with submitting, viewing, accessing, using, disclosing and exchanging, and retrieving Client Data for the purpose of providing treatment, payment, healthcare operations, public health, reporting as permitted or required by Applicable Law, the determination of eligibility for government or other benefits, care coordination including information and referral and program enrollment assistance or other activities performed for or on behalf of a Client or Participant and as otherwise permitted by Applicable Law.
- 1.3.21 “Person”** means an individual person, an entity or a governmental organization or agency, including health and/or community information exchanges, researchers, Participants, and/or an individual(s) who does not participate in the Database.
- 1.3.22 “PPRA”** means the Protection of Pupil Rights Amendment and its implementing regulations promulgated thereunder at 34 C.F.R. Part 98, as amended.
- 1.3.23 “Security Breach”** means (1) the failure to properly secure, transmit, handle, manage, store, backup, destroy or otherwise control, or the unauthorized use or disclosure of: (a) Data in any format, or (b) third party proprietary information in any format specifically identified as confidential and protected under a confidentiality agreement or similar contract; (c) a violation of the privacy policy, (d) violation of Applicable Laws, including but not limited to a Security Incident or Breach under HIPAA; or (2) any other act, error, or omission that is reasonably likely to result in the unauthorized disclosure of Data.
- 1.3.24 “System Data”** means each and collectively Client Data, aggregated, and/or de-identified data that is collected, created, maintained, or disclosed by VCCIE.

2.0 PARTICIPATION IN VENTURA COUNTY COMMUNITY INFORMATION EXCHANGE.

- 2.1 Non-Discrimination and Equal Access.** Each Party shall administer its activities under this Agreement, including participation in and operation of the Community Information Exchange and use and operation of the Database, in a manner that proves equal access to eligible Clients and does not discriminate on the basis of race, color, religion, sex, gender, gender identity, sexual orientation, national origin, age, disability, or any other characteristic protected by applicable law. Participant will ensure that its Authorized Users and personnel administering referrals and services for Clients through the Database do so in a non-discriminatory manner consistent with Applicable Law.



PHASE I PILOT PARTICIPATION AGREEMENT

2.2 Client Data: Ownership, Use, License and Quality.

2.2.1 VCCIE's Use of Client Data. Subject to the limitations on the use of System Data in any applicable Policies and Procedures (defined below) and Applicable Law, the Participant grants the VCCIE a fully paid, royalty-free, non-exclusive, nontransferable right and license: (a) to permit Persons to access through the Database and/or to receive from the Database all Client Data provided by the Participant; (b) to use Client Data provided by Participant to perform any activities VCCIE is allowed to perform under the Agreement (including any applicable Policies and Procedures); (c) to use Client Data provided by Participant to carry out VCCIE's duties under the Agreement, including system administration, testing and audits, provision of services, problem identification and resolution and management of the Database; (d) to release data in accordance with any applicable Policies and Procedures, the BAA, and as permitted or required by Applicable Law; and (e) to facilitate the access of an individual and his/her/their personal representatives to the individual's data in accordance with any applicable Policies and Procedures, the BAA, and as required by Applicable Law. VCCIE's rights under this Section 2 will continue for as long as VCCIE holds or controls Participant's Client Data.

2.2.2 Participant Access to Database. The VCCIE grants to Participant, and Participant accepts, a non-exclusive, personal, nontransferable, limited right to access and use the Database under the terms and conditions set forth in the Agreement. Participant's right is conditioned on Participant fully complying with the Agreement. Participant does not have any other right to access the Database unless otherwise expressly granted by the Agreement or a separate written arrangement that complies with Section 2.2.3 below. VCCIE retains all other rights to the Database and all the components thereof.

2.2.3 Participant Use of System Data.

2.2.3.1 When accessing or using System Data pursuant to the Agreement, Participant and its Authorized Users (defined below) may access and/or use System Data to send, receive, and track referrals and otherwise provide services to Clients as authorized under the Agreement (including any applicable Policies and Procedures) and



PHASE I PILOT PARTICIPATION AGREEMENT

the BAA.

2.2.3.2 Notwithstanding any other provision of the Agreement, if Participant or its Authorized User(s) accesses any System Data that it is not permitted to access under the Agreement at the time of such access, then Participant: (a) will be in breach of the Agreement, (b) will not have or obtain any right to that System Data, and (c) must immediately return or destroy that System Data and any copies thereof, at VCCIE's sole discretion.

2.2.4 No Limitation of Participant's Use of Its Own Data. Nothing in this Section 2 or elsewhere in the Agreement is intended or will be deemed to limit Participant's use of its own data for its own legal purposes.

2.2.5 VCCIE and VCCIE Vendor's(s') Trademarks. The Participant and its employees, agents, representatives, and contractors must: (a) maintain VCCIE's and VCCIE vendor's(s') copyright notices and legends, proprietary markings, trademarks, marks, service marks, tradenames, or logos; and (b) not violate VCCIE's and/or VCCIE vendor's(s') copyright notices and legends, proprietary markings, trademarks, marks, service marks, tradenames, logos, and/or any other intellectual property rights. Participant will be liable for the acts of third party service providers engaged by Participant who violate these proprietary rights or related law.

2.2.6 Revocable License to Display Trademark/Logo. The Parties hereto grant the other a fully-paid, non-exclusive, royalty-free, nontransferable right and license to display the other's trademarks, marks, tradenames and logos on its website and on other media in connection with the Party's efforts to educate the general public, Clients, and other existing and potential Participants about the Participant's enrollment with the VCCIE and the benefits of participating in the program. Upon termination, all rights and license to display the trademarks, marks, tradenames and logos of the other Party shall immediately terminate. The Parties agree that neither Party will use the trademarks, marks, tradenames and logos of the other Party in a manner that would be misconstrued as an endorsement of the services or products of the other Party.

2.3 Participation Policies and Procedures. The VCCIE may adopt, amend, repeal, and replace rules, definitions, guidelines, and/or standards which

PHASE I PILOT PARTICIPATION AGREEMENT

are published by VCCIE to Participants to facilitate the compliant use and administration of the Database (“Policies and Procedures”). The Policies and Procedures will provide guidance to Participants concerning topics such as but not limited to security measures required to protect Client Data, immediately notifying the VCCIE in the event the Participant experiences a known or suspected Security Breach (as defined herein), referral acceptance/rejection response times, and outcome reporting requirements, among other things. VCCIE Policies and Procedures will be available and accessible in a web-supported format and are hereby incorporated in this Agreement by this reference as if fully set forth herein. The VCCIE may modify, amend, or replace the Policies and Procedures, in its reasonable discretion, from time to time, and the change or modification shall be deemed effective and binding upon the Participant on the date indicated, but not less than thirty (30) days from the date the Participant receives the modified Policies and Procedures. Material modification to the Policies and Procedures shall require the prior approval of the VCCIE Board of Directors. In the event the VCCIE adopts a new, or modifies an existing, policy or procedure in a way that materially changes the Participant’s obligations, liability, or ability to participate in the Database, then the Participant may terminate this Agreement as provided below. Modifications to the Policies and Procedures that are required by Applicable Law shall not be deemed a material change and will be adopted and implemented by the Participant as soon as possible and practicable.

2.4 Participants’ Information and Client Data.

- 2.4.1** It is the responsibility of the Participant to use reasonable care to ensure the accuracy, currency, and completeness of the Participant’s profile and directory information within the Database. Participants are cautioned that VCCIE does not independently validate the information provided by Participants or made available to Participants via access to the Database; the VCCIE does not assume any responsibility or liability for any inaccuracies.
- 2.4.2** To the extent that Client Data is entered into the Database by the Participant (which excludes, for example, information entered or modified by a Client and not reported to the Participant for the Participant to enter), such Client Data of the Participant, including Client demographic information, shall be promptly corrected or updated when the Participant becomes aware that any Client Data

PHASE I PILOT PARTICIPATION AGREEMENT

are incorrect, incomplete or have otherwise changed. Collectively, all Client Data, both self-reported and provided by the Participant, along with the Participant profile and directory information, is hereinafter referred to as “Data”.

- 2.4.3** The VCCIE does not assume any responsibility or liability for the accuracy and reliability of any of the Data contained within the Database; and Client Data are not a substitute for the source records (such as medical records) and/or any other source of information from which Client Data is derived.

2.5 Participants’ Responsibilities with Respect to Authorization.

Participant is solely responsible for:

- 2.5.1** Obtaining and confirming the Authorization of a person who desires to benefit from the VCCIE.
- 2.5.2** Confirming the valid Authorization of a person who has already provided an Authorization to benefit from the VCCIE.
- 2.5.3** Receiving a revocation of an Authorization in the event that a Client no longer wishes to be engaged with the VCCIE and notifying the VCCIE immediately of such revocation or any other changes or restrictions to an Authorization.
- 2.5.4** Cooperating, when required by Applicable Law, to disclose Protected Health Information to the VCCIE and other Participants;
- 2.5.5** Protecting Client Data within the possession or control of the Participant from any unlawful use or unauthorized disclosure;
- 2.5.6** Notifying the VCCIE immediately of any suspected or known Security Breach involving Client Data or the Database; and
- 2.5.7** Maintaining role-based access to the Database, meaning the Participant shall not disclose to, or receive from, another Participant or the VCCIE, Client Data retrieved from the Database unless the Participant is authorized to do so, by Authorization and/or as a matter of law.

2.6 Participation Scope.

- 2.6.1** The Participant shall not use or disclose, or permit others to use or disclose, Client Data or access the Database for any purpose other than to provide the types of services described in the Participant’s profile as published in the Database, to refer a Client to another Participant, or for any other lawfully permitted use in compliance with the Authorization, BAA, and all Applicable Laws.
- 2.6.2** The Participant shall not sell, view, access, use, download or



PHASE I PILOT PARTICIPATION AGREEMENT

disclose Client Data retrieved from the Database, except to the extent necessary and consistent with the Authorization, and as necessary to provide services and allow for payment for services provided by the Participant to a Client.

- 2.6.3** The Participant shall not provide access to the Database or to Client Data, via or obtained from the Database, to third parties who are not Participants of the Database or use or disclose Client Data in connection with any marketing, fundraising, or other activity not permitted by Applicable Laws.

3.0 PARTICIPANT'S USE OF THE DATABASE.

3.1 Minimum Necessary Use of Client Data. Whether Client Data is obtained through the Database, or directly from the VCCIE or another Participant, the Participant shall implement safeguards to limit the information accessed, retrieved, or requested to the minimum necessary to deliver and obtain payment for the services provided to the Client, for referral or for other lawful purposes consistent with the Authorization, BAA, and Applicable Law. The minimum necessary standard discussed here does not apply to:

- (a) Disclosures to or requests by a health care provider for treatment purposes;
- (b) Disclosures to the Client who is the subject of the information to be disclosed;
- (c) Uses or disclosures made pursuant to the Client's express authorization;
- (d) Uses or disclosures required for compliance with HIPAA;
- (e) Disclosures to the Department of Health and Human Services when disclosure is required under HIPAA for enforcement purposes; and
- (f) Uses or disclosures that are otherwise required by law.

The Parties acknowledge and agree that Participants may share or disclose data outside of the Database that matches some or all of a Client's Client Data contained within the Database pursuant to a separate agreement or arrangement that is not governed or otherwise limited by this Agreement; provided, however, the Parties further agree that such agreement or arrangement shall be done in accordance with Applicable Laws and any such disclosure is not otherwise authorized by this Agreement.

3.2 Web-Services Participants. Internet Connection to the Database. The Participant, at the Participant's sole cost and expense, will use



PHASE I PILOT PARTICIPATION AGREEMENT

commercially reasonable efforts to obtain and maintain a secure internet connection to the Database with an internet browser and computer equipment and software that meets or exceeds the minimum configuration and security requirements and specifications recommended by the VCCIE. The Participant will be permitted access to the Database and segments of Client Data according to the Participant type and data access permissions assigned to the Participant's Authorized Users by logging onto the VCCIE web portal using the Participant's unique logon credentials.

- 3.3 Authorized Users.** An Authorized User is an employee or agent of VCCIE and/or a Participant whose capacity as such involves access and use of the Database for authorized purposes including, for example, Client support or Database maintenance. A Participant shall limit access to the Database to that number of Authorized Users equal to or less than the number of Database licenses granted to the Participant ("User Licenses"). User Licenses will be renewed on a calendar year basis (each calendar year "User License Term").

3.3.1 The Participant shall conduct ongoing monitoring of the User Licenses to ensure that the number of Authorized Users registered under the Participant to use the Database does not exceed the number of User Licenses issued. The Participant shall train its Authorized Users on the proper use of Client Data and the means and methods for protecting Client Data from unlawful disclosure before allowing such Authorized User to access the Database.

3.3.2 The Participant shall implement and train its Authorized Users on network privacy and cultural competence on a regular basis, not less than annually.

3.3.3 The Participant shall immediately notify the VCCIE and the vendor issuing the end user license (such vendor hereinafter "Database Vendor") of any changes to an Authorized User's status or access rights.

- 3.4 Participant Security Requirements.** The Participant shall, at its sole cost and expense, implement, maintain and update as needed, internal security systems, specifications and monitoring procedures to ensure that its computer servers, software and internet connections meet or exceed the security standards and specifications established by the VCCIE and Applicable Law, and regularly monitor its own electronic record database, systems, and personnel, to the extent that each interface or otherwise

PHASE I PILOT PARTICIPATION AGREEMENT

engage with the Database, to protect the privacy and security of Client Data in compliance with this Agreement and Applicable Laws.

3.5 Participant's Responsibilities of Database Access and Use, Documentation. The Participant shall not and shall not allow others to:

- 3.5.1** Interfere with or disrupt the Database;
- 3.5.2** Sell, assign, license, sub-license or otherwise provide access to the Database or documentation related to the Database to anyone other than those employees, agents or contractors who have a need to know (i.e., "Authorized User");
- 3.5.3** Use the Database or its documentation or Client Data for the purposes of providing commercial use in a service bureau, timesharing, remote batch, or similar commercial operations with third parties;
- 3.5.4** By reverse engineering or by other process, create or attempt to create, or recreate the Database;
- 3.5.5** Copy, modify, or distribute any portion of the Database or any documentation related to the Database or Client Data other than in connection with the delivery of services or referral of Clients to other Participants; provided, however, that the Participant may make and use copies of the System Data for archival and back-up purposes solely to the extent authorized by Applicable Law;
- 3.5.6** Transfer or assign any of its rights hereunder;
- 3.5.7** Create any derivative works based on the Database or its documentation; or
- 3.5.8** Export, re-export, divert, or transfer the Database or its documentation outside of the United States.

3.6 Participant Profile. The Participant shall ensure the Database contains up-to-date registration and profile information that accurately describes the programs and services offered by the Participant to eligible VCCIE Clients, eligibility requirements for such programs and services, and contact information for processing referral requests submitted to the Participant by other Participants and/or Clients through the Database.

3.7 Referral Requests. The VCCIE shall not be required to refer Clients to the Participant ("Referral Requests"). In the event a Client is referred to the Participant through the VCCIE, the referral-receiving Participant shall promptly respond to a Referral Request in the manner and within the timeframe specified by the VCCIE in the Referral Request or as otherwise specified in any applicable Policies and Procedures. If no timeframe is



PHASE I PILOT PARTICIPATION AGREEMENT

specified, the Participant shall respond to the Referral Request within that number of days then established in the Participant's own written policies and procedures. If the timeframe is not specified within the Participant's own written policies and procedures, then the Participant shall respond within a timeframe commensurate with the prompt resolution of the Client's need and attributable priority. The Participant's failure to respond to a Referral Request three times in any consecutive four-week period shall initiate an opportunity for the VCCIE and the Participant to meet to discuss timeframes.

4.0 ADMINISTRATION OF THE DATABASE.

4.1 Database Operations. The VCCIE will:

4.1.1 Maintain and operate the Database which may involve contractors and agents working on behalf of VCCIE, including maintenance and operation of the Participant directory and profile and Client Data, as well as facilitation of the electronic storage and exchange of Client Data between and among Participants in accordance with Authorizations; in the event that VCCIE engages contractors or agents for maintenance and/or operations, VCCIE will require these contractors or agents to:

4.1.1.1 Maintain the confidentiality of all Client Data and other proprietary and confidential information relating to the Participant;

4.1.1.2 Execute a Business Associate Agreement with, at a minimum, the same restrictions and conditions that apply to the VCCIE, if applicable, whenever such person or entity may have access to, view, receive, transmit or disclose protected health information;

4.1.1.3 Implement security measures to protect Client Data for unlawful use or disclosure; and

4.1.1.4 Require its contractors, employees, and agents to comply with all Applicable Laws.

4.1.2 Provide user support, through its vendor, to the Participant and its Authorized User(s) via a helpdesk;

4.1.3 Ensure Database compliance with Applicable Law and regulations.

4.1.4 Upgrade the Database from time to time to ensure operability, and provide support services.

4.2 Level of Access and Administration of Access. To protect the privacy and security of Client Data, the VCCIE may restrict Participant access to

PHASE I PILOT PARTICIPATION AGREEMENT

the Database in accordance with the service profile of the Participant and the informational needs associated with eligibility and service delivery to Clients. Participants entered into this Agreement by selecting and accepting terms and conditions appropriate to their access to and use of the Database. VCCIE reserves the right to adjust Participants' level of access to the Database at any time including, for example: (a) to affect a revocation of an Authorization that permits VCCIE to hold Client Data, or (b) to reduce the risk associated with a Participants' access, which includes when a Participant does not have sufficient insurance for a particular access level as required in Section 9.0 below. Each Participant and Authorized User will hold permissions and have access as appropriate based on its organization, user type, and role the Authorized User serves for the Participant, respectively. The specific organization types and roles may be found in the Policies and Procedures and may be modified and amended in accordance therewith.

- 4.3 Database Availability.** The VCCIE shall operate and maintain the Database in a manner consistent with commercially reasonable industry standards relevant to the VCCIE. The VCCIE shall provide the Participant with Database access for 98% of the minutes within a given month, 24 hours per day, 7 days per week during the Term, excluding pre-scheduled maintenance windows and excluding up to 2 hours per month of Emergency Maintenance, such maintenance discussed in greater detail below. The Database will be subject to downtime, planned and unplanned, and to the extent reasonably possible, (except in the event of Force Majeure and Global Pandemic), Database Vendor will provide advance written notice of downtime(s) by sending the Participant a downtime alert by email, or VCCIE will provide notice by posting the information on the VCCIE website. Notwithstanding the foregoing, the Participant acknowledges and agrees that the Database's availability is provided on an "As Is, As Available" basis.

4.3.1 Pre-scheduled Maintenance, which is maintenance performed one to two days every month on a pre-scheduled basis in accordance with Database Vendor's published terms and procedures, which may change from time to time to balance operational and maintenance needs, and will typically last ten minutes or less.

4.3.2 Other Maintenance, which is pre-scheduled maintenance for which Database Vendor will provide advance notice ranging from

PHASE I PILOT PARTICIPATION AGREEMENT

24 to 96 hours depending on the length of downtime required, will typically last for less than 30 minutes at a time for less than 3 hours per month, and will not require more than 3 hours of downtime for any individual instance. Other Maintenance can occur any day of the week but will be during such time stated in the notice provided by Database Vendor.

4.3.3 System-wide Maintenance, which is pre-scheduled maintenance for which Database Vendor will strive to provide four weeks' advance notice and may be performed for up to eight hours at no more than two times in a twelve-month period. System-wide Maintenance will be performed overnight to reduce disruption to normal operations.

4.3.4 Emergency Maintenance, which is maintenance for which advance notice will not be provided and that is performed when deemed appropriate by Database Vendor, balancing the disruption to users with the security and integrity of the system. If Emergency Maintenance results in no downtime for users, then no notice will be given. Information about Emergency Maintenance that results in downtime for users will be given as soon as reasonably possible after the maintenance begins and updates on the status will be provided in 15-minute increments until complete.

4.4 Accessibility. VCCIE will perform its obligations under this Agreement such that the Database provided hereunder (including, but not limited to any: software applications and operating systems; Web-based internet information and applications, information, documentation and support; desktop and portable computers; video and multimedia products; self-contained, closed products; and telecommunication products) are usable by a person with a disability in accordance with Title III of the Americans with Disabilities Act, 42 U.S.C. § 12181, et seq., and/or Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. §§ 701, et seq., and Section 1194.22(a) - (p) of the Electronic and Information Technology Accessibility Standards, 36 C.F.R. Part 1194 (implementing Rehabilitation Act Section 508 (29 U.S.C. § 794d)), and/or Section 1557 of the Affordable Care Act, 42 U.S.C. 18001, et seq. (2010) and its implementing regulations, and are in compliance with WCAG 2.0 (Web Content Accessibility Guidelines) standards.

4.5 Upgrades or Modifications to Connection Specifications. The VCCIE may upgrade or adopt new or different specifications for connecting to the



PHASE I PILOT PARTICIPATION AGREEMENT

Database from time to time and will notify the Participant of any material changes to its specifications not less than thirty (30) days in advance if feasible. The VCCIE shall not be liable for any lack of connectivity or loss in functionality in the event the Participant utilizes hardware or software or an internet browser that does not meet VCCIE recommended specifications.

- 4.6 Database Records.** The VCCIE will maintain records, in the form of a HIPAA compliant Data access log, of the dates, times, and the specific Client records accessed by Authorized Users if, as and for the period of time required by Applicable Law. Within thirty days of a written reasonable request, the VCCIE will provide Participant a copy of the Data access audit log.
- 4.7 Security of Client Data.** The VCCIE shall establish, implement, and maintain commercially reasonable security measures to ensure the privacy and security of Client Data while at rest in the Database and during its transmittal to and from Participants through the Database.
- 4.8 Disaster Recovery.** The VCCIE will establish, implement, and update a disaster recovery plan which addresses the retrieval of lost, or corrupted Client Data in the event of Force Majeure, or a known or suspected Security Breach. Notwithstanding the foregoing, the VCCIE shall not be liable, under any theory, for lost, corrupted, irretrievable, inaccurate, or incomplete Data; except, however, to the extent that VCCIE's disaster recovery plan fails to meet community information exchange industry standards.

5.0 PAYMENT.

- 5.1 Consideration.** During the term of this Agreement, the VCCIE will offer access to, and offer services related to, the Database, as consideration for Participant's use of, and dependent upon the Participant's level of access to, the Database, the Participant shall provide such support, reports, and insights to the VCCIE, at such times and intervals, as deemed necessary by a committee consisting of one representative from each of the Participants in accordance with VCCIE's Policies and Procedures. The VCCIE reserves the right to establish any fees it deems fit during or after the expiration of the Pilot Period (defined below), which will be defined and memorialized in a separate written agreement signed by both Parties, to the extent applicable.
- 5.2 Taxes.** The Parties will each be solely responsible for all of their own respective tax returns and payments required to be filed with or made to



PHASE I PILOT PARTICIPATION AGREEMENT

any federal, state, or local tax authority with respect to each Party's performance of services under or related to this Agreement. The VCCIE will not be responsible for and will have no obligation to the Participant, its clinicians, or any other personnel of the Participant or any governing body to withhold federal, state, or local income tax, or any portion of FICA or other payroll taxes, and other taxes relating to any clinician or Participant personnel performing hereunder.

6.0 **WARRANTY DISCLAIMER, CARRIER LINES LIABILITY.**

6.1 Warranty Disclaimer. The VCCIE is not responsible for and shall not be liable for the content, use or disclosure of Client Data collected, stored, accessed, retrieved, or transmitted through the Database to or from a Participant; except to the extent that such use or disclosure arises from VCCIE's negligent or willful misconduct or omissions. The Participant acknowledges that the Client Data viewed or accessed through the Database is presented as secondary records. Client Data are not a substitute for the source records (such as medical records) and/or any other source of information from which Client Data is derived. Client Data may be self-reported by the Client and/or entered into the Database by a Participant; such Client Data may not be complete, accurate, or up-to-date. The Participant and its Authorized Users are solely responsible for confirming the completeness, accuracy, and timeframe of all Client Data, as needed for the Participant's use or omission of such Client Data in connection with a Client's care or coordination of care and/or related services. The VCCIE will use commercially reasonable efforts to make Client Data available to the Participant if, when, and to the extent the Database software is able to match up the records for such Client in the electronic record database or systems of other Participant(s) and to notify Participant(s) whenever it discovers duplicate or inappropriately linked Client records. Access to the Database, the Database itself, and the Data viewed or retrieved therefrom is licensed "As Is" and "As Available." The VCCIE disclaims all representations and warranties of any kind as they may pertain to the functionality of the Database or the accuracy, completeness or timeliness of the Data including, without limitation, any implied warranty of merchantability or fitness for a particular purpose.

6.2 Internet Security and Carrier Lines. The Participant acknowledges that access to the Database will be provided over various telecommunications facilities and lines, and that Data may be transmitted over local exchange and internet carrier lines and through routers, switches, and other devices



PHASE I PILOT PARTICIPATION AGREEMENT

owned, maintained, and serviced by third-party carriers, utilities, and internet service providers (collectively, “carrier lines”), all of which are beyond the VCCIE’s and the Participant’s control. Neither the VCCIE nor the Participant shall be liable for the integrity, privacy, security, confidentiality, and use of Data as it transits carrier lines, or for any delay, failure, interruption, interception, loss, transmission, or corruption of any Data attributable to transmission on the carrier lines. Notwithstanding the foregoing, the Parties agree to take commercially reasonable steps to ensure that the exchange of Client Data shall be encrypted in transit to prevent an unauthorized disclosure of such Client Data transferred over carrier lines.

7.0 RELEASE AND LIMITATION OF LIABILITY.

7.1 RELEASE OF LIABILITY. THE PARTICIPANT IS SOLELY RESPONSIBLE FOR AND HEREBY RELEASES THE VCCIE, ITS OFFICERS, DIRECTORS, EMPLOYEES, CONTRACTORS, AND AGENTS OF AND FROM ALL LIABILITY ARISING OUT OF ANY AND ALL ACTS OR OMISSIONS, TAKEN OR MADE BY THE PARTICIPANT, IN RELIANCE ON THE DATABASE, CLIENT DATA, DISCLOSURE OF CLIENT DATA, OR THE FAILURE OF THE PARTICIPANT TO OBTAIN A CLIENT’S CONSENT OR AUTHORIZATION TO DISCLOSE A CLIENT’S DATA TO THE VCCIE AND OTHER PARTICIPANTS WHEN REQUIRED TO DO SO UNDER APPLICABLE LAW. FURTHERMORE, THE PARTICIPANT IS SOLELY RESPONSIBLE FOR AND HEREBY RELEASES THE VCCIE, ITS OFFICERS, DIRECTORS, EMPLOYEES, CONTRACTORS, AND AGENTS OF AND FROM ALL LIABILITY OR CLAIMS ARISING OUT OF OR RELATED TO THE ACCURACY OF CLIENT DATA WITHIN THE DATABASE.

7.2 LIMITATION OF LIABILITY. EXCLUDING CLAIMS FOR INDEMNITY IN SECTION 8, AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, the Parties agree that VCCIE’s aggregate liability to the Participant, regardless of theory of liability or characterization of damages, will be limited to \$1,000,000.00. The Parties further agree that they will not be liable to one another for any consequential or indirect damages, including but not limited to lost profits, lost wages, or emotional damages, which may arise from any dispute, claim, cause of action, or any other liability.

8.0 INDEMNIFICATION; RESPONSIBILITY.

8.1 Each Participant shall indemnify, defend and hold VCCIE and any other

PHASE I PILOT PARTICIPATION AGREEMENT

Participant harmless (each when indemnifying another is hereinafter referred to as the “Indemnitor”) from and against any damages, cost or expense, net of the proceeds of insurance, incurred by the other (the “Indemnitee”) for third party claims resulting from a Security Breach caused solely by the Indemnitor’s acts or omissions, whether or not negligent or intentional. Any indemnification provided under this Section 8.1 where the Indemnitor is indemnifying another Participant shall be limited to the maximum insurance coverage amount held by the Indemnitor; provided, however, only to the extent the Indemnitor is maintaining insurance at or above those levels established in Section 9 below.

- 8.2** Each Participant providing Client Data hereunder acknowledges and agrees that it is responsible for damages arising out of Participant’s provision of Client Data that is not accurate, not free from serious error, materially incomplete, or defamatory. To the extent that Participant is responsible for obtaining an authorization to allow VCCIE to provide access to Client Data to other Participants, Participant agrees to be responsible for damages arising out of Participant’s provision of Client Data. Nothing within this Section 8.2 will, nor will be interpreted to, impose on any Party an obligation to indemnify or defend another Party under this Section 8.2.
- 8.3** Any indemnification made pursuant to this Section 8 (Indemnification) shall, unless otherwise provided, include payment of all costs associated with defending the claim or cause of action involved, whether or not such claims or causes of action are meritorious, including reasonable attorneys’ fees and any settlement by or judgment against the Indemnitee. In the event that a lawsuit is brought against the Indemnitee, the Indemnitor shall, at its sole cost and expense, defend the Indemnitee, if the Indemnitee demands indemnification by written notice given to the Indemnitor within a period of time wherein the Indemnitor is not prejudiced by lack of notice. Upon receipt of such notice, the Indemnitor shall have control of such litigation but may not settle such litigation without the express consent of the Indemnitee, which consent shall not be unreasonably withheld, conditioned or delayed. The indemnification obligations of the parties shall not, as to third parties, be a waiver of any defense or immunity otherwise available, and the Indemnitor, in indemnifying the Indemnitee, shall be entitled to assert in any action every defense or immunity that the Indemnitee could assert on its own behalf.



PHASE I PILOT PARTICIPATION AGREEMENT

9.0 INSURANCE.

9.1 Participant's Insurance. Unless otherwise agreed, the Participant, at its sole cost and expense, shall obtain and keep in force, such professional, general, and cyber liability insurance policy or policies, or self-insure, in an amount Participant deems reasonable and necessary to insure itself and its officers, directors, employees, and contractors against any third-party claims or causes of action arising out of the performance of this Agreement. Such policies shall provide, at minimum, coverage of the following types and amounts set forth below and in each case waiving the right of the insurer to subrogation, during the term of this Agreement and for three (3) years thereafter, or shall provide an equivalent extended reporting endorsement or tail policy.

9.1.1 Comprehensive or Commercial Form General Liability. Blanket contractual liability, broad form property damage, personal injury included, with minimum limits as follows: (a) each occurrence \$1,000,000 limit, (b) products/completed operations aggregate \$2,000,000 limit, (c) personal and advertising injury \$1,000,000 limit, (d) professional liability \$1,000,000 limit, (e) cyber liability with extortion coverage \$500,000 limit, and (f) general aggregate \$3,000,000 limit.

9.2 Access Limitation. Should a Participant choose not to maintain the minimum coverage limits required above, then that Participant's permissions, regardless of Participant's organization type, or user type or role, will be reduced to allow for limited access to only those aspects of the Database necessary to receive and send referrals and query the service directory. Participant's permissions will only be elevated at such time that it is able to provide proof of coverage sufficient to meet the limits above.

9.3 Additional Insurance Requirements. Participant shall provide proof of the coverage above and additional insured endorsements promptly upon receipt of a written request from VCCIE.

9.4 VCCIE Insurance. The VCCIE shall obtain, at its sole cost and expense, and keep in force, at all times during the Term of this Agreement, insurance for "cyber-liability" or other similar insurance appropriate for a breach of personal health information, as well as such professional and general liability insurance policy or policies, or self-insurance in an amount VCCIE deems reasonable and necessary to insure itself and its officers, directors, employees, and contractors against any third-party claims or



PHASE I PILOT PARTICIPATION AGREEMENT

causes of action arising out of the performance of this Agreement. Such policies shall provide, at minimum, the above coverage during the term of this Agreement and for three (3) years thereafter, or shall provide an equivalent extended reporting endorsement or tail policy.

10.0 TERM AND TERMINATION.

10.1 Term of Agreement. This Agreement shall be in effect for an initial period of three (3) years ("Pilot Period"), effective as of the last date of the signatures below ("Effective Date"), unless terminated earlier as provided herein.

10.2 Termination by Participant. The Parties reserve the right to terminate this Agreement in whole or in part without liability at any time and without cause, upon thirty (30) days' prior written notice to the other Party.

10.3 Termination by VCCIE.

10.3.1 Privacy and Security. VCCIE may in its sole discretion terminate the Agreement at any time if VCCIE determines in its sole discretion that Participant's actions and/or continued participation in VCCIE would, or is reasonably likely to, endanger the privacy or security of Client Data or otherwise result in a breach of the Agreement that is reasonably likely to harm VCCIE or another Participant. VCCIE shall deliver notice of this termination to Participant at least twenty-four (24) hours prior to terminating Participant's access to the Database, unless VCCIE determines in its sole discretion that Participant's access must be terminated immediately in order to protect the privacy or security of the Client Data, in which case VCCIE may terminate access immediately without notice.

10.3.2 Cessation. VCCIE may terminate this Agreement after providing sixty (60) days' written notice to Participant that VCCIE will discontinue its operations and/or its provision of the Database to Participants.

10.3.3 Uncured Breach. VCCIE may terminate the Agreement if Participant breaches the Agreement and that breach continues uncured for a period of thirty (30) days after VCCIE has delivered written notice of that breach to Participant. VCCIE's notice of breach shall include a description of the breach.

10.3.4 Termination for Insolvency/Bankruptcy. VCCIE may terminate this Agreement as a result of (i) the institution by or against the Participant of insolvency, receivership or bankruptcy proceedings or



PHASE I PILOT PARTICIPATION AGREEMENT

any other proceedings for the settlement of the Participant's debts,
(ii) the Participant making an assignment for the benefit of creditors,
or (iii) the Participant's dissolution or ceasing to do business.

10.4 Effect of Termination on Client Data. Upon any termination of this Agreement, Participant shall cease to be a Participant and thereafter neither the former Participant nor its Authorized Users shall have any rights to use the Database or receive any services related to the Database. Participant shall have no obligation to provide data following the termination of this Agreement. All licenses or other rights to use the Database, and access Client Data therein, granted to the Participant hereunder shall terminate automatically upon the termination of this Agreement. The PII and Protected Health Information to which VCCIE will have access by virtue of Participant's participation in the Database is necessary to the ongoing operation of the Database in support of all the other Participants. As such, if Participant has provided Client Data to VCCIE, the Parties acknowledge and agree that such Client Data and/or Participant data has been merged with VCCIE's and/or other Participants' data and, accordingly, it is infeasible to destroy, delete, or return such data. The terms of the BAA shall continue to apply to the applicable Participant provided Client Data until the data is returned or destroyed in accordance with Applicable Laws. Both Parties must continue to protect any Client Data that it possesses provided by another Party or Participant so long as such Client Data is within that Party's possession. Certain provisions of this Agreement shall continue to apply to Participant and its Authorized Users following termination, as described in Section 11.13 below.

11.0 GENERAL PROVISIONS.

11.1 No Exclusion. The Parties each warrant and represent that neither they nor any of their Related Parties have been placed on the sanctions list issued by the office of the Inspector General of the Department of Health and Human Services pursuant to the provisions of 42 U.S.C. 1320a(7), or have been excluded from government contracts by the General Services Administration. A Party will provide the other immediate notice in the event either is placed on the sanctions list.

11.2 Severability. If any provision of this Agreement is determined to be invalid or unenforceable, such provision shall be changed to best accomplish the objectives of the Parties within the limits of Applicable Law, provided, however, if that is not possible or feasible, such provision will be severed

PHASE I PILOT PARTICIPATION AGREEMENT

from this Agreement to the extent of such determination without affecting the validity or enforceability of such remaining provisions.

- 11.3 Governing Laws.** This Agreement is governed by and shall be interpreted in accordance with the laws of the State of California without regard to its conflict of law provisions. The Parties waive any objections and agree to the venue and personal jurisdiction of the courts of the State of California and the federal courts situated in Ventura County over any action arising out of or relating to this Agreement.
- 11.4 Force Majeure.** No Party shall be liable to the other for any failure to perform its obligations under this Agreement, where such failure results from any act of God or other cause beyond such Party's reasonable control, including, without limitation, any mechanical, electronic, or internet communications failure, terrorist acts, cyber terrorism, or malicious mischief.
- 11.5 Assignment.** Neither Party may assign the Agreement or any of such Party's rights, interests, duties or obligations under the Agreement, by operation of law or otherwise, without the prior written consent of the other Party, which consent may be given, conditioned, or withheld in the other Party's sole discretion, except that (a) either Party may assign the Agreement in whole or in part to an affiliate or to a successor in interest, and (b) consent shall not be necessary in the context of an acquisition, merger, or change of control involving either Party. Any attempted assignment or transfer in violation of the foregoing will be null and void.
- 11.6 Notices.** Except as otherwise provided herein, all notices, requests, demands, and other communications required or permitted by this Agreement (collectively and each individually hereinafter "Notice") will be in writing and shall be deemed to have been duly given, made and received on the date when delivered to the other Party at the address stated below the signature line when actually delivered by a nationally recognized courier service, or on the third business day following the day when deposited in the United States mail, certified, postage prepaid, return receipt requested. A Party may change its address for Notice, at any time, by giving Notice of such change as provided herein. The Parties may send a courtesy copy of any Notice through email or other electronic means, but such emailed Notice shall not constitute official Notice hereunder and must be sent only in conjunction with an effective Notice process addressed above.
- 11.7 No Agency, No Third-Party Beneficiaries.** The VCCIE provides the

PHASE I PILOT PARTICIPATION AGREEMENT

Database services to the Participant but does not act as the Participant's agent. The Participant will not be deemed an agent of another Participant as a result of participation in the Database. In all cases, VCCIE will be acting as an independent contractor, and nothing contained herein may be construed to create a partnership or a joint venture or to authorize either Party to act as a general or special agent of the other Party. Nothing in this Agreement is intended to confer upon any third party any rights, remedies, or obligations.

- 11.8 Modifications.** Except as specifically provided herein, no modification to the terms of this Agreement or the BAA shall be valid, unless in writing and signed by the respective authorized signatories of the Parties hereto.
- 11.9 Authorized User Signatures and Signed Documents.** Upon registering with the Database, the Participant acknowledges and agrees that its Authorized User is authorized to adopt as its signature an electronic identification consisting of symbols or codes that are to be affixed to or contained in an exchange of Data made by the Participant ("Signatures"). Any transmission or exchange of Data made pursuant to this Agreement shall be considered a "writing" or "in writing" and any such exchange when containing, or to which there is affixed, a Signature shall be deemed for all purposes: (a) to have been "signed" ("Signed Documents") and (b) to constitute an original when printed from electronic files or records established and maintained in the normal course of business. The Participant will not contest the validity or enforceability of Signed Documents under the provisions of any Applicable Law as they may relate to the requirement that certain agreements be in writing or signed by the party to be bound thereby. Signed Documents, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings will be admissible as between the Parties to the same extent and under the same condition as other business records originated and maintained in paper form.
- 11.10 Complete Agreement.** The terms of this Agreement and its Attachments and Exhibits collectively represent the entire understanding between the Parties and supersede all previous agreements, whether oral or in writing, as they relate to the subject matter hereof. The Attachments and/or Exhibits attached to this Agreement and identified in the Summary box on page one, are fully incorporated and made a part of this Agreement by this reference as if fully stated herein.
- 11.11 No Additional Terms.** No online "click to accept" agreement that may be

PHASE I PILOT PARTICIPATION AGREEMENT

required for the Participant or any of the Participant's end-users to access or utilize the Database and no "terms of use", "privacy policy", "end user license agreement" or any other VCCIE terms and conditions referenced therein or upon which access to or use of the Database is conditioned shall apply (and even if the Participant or the Participant end-users are required to accept any such additional terms in order to access or utilize the Database as a Participant, the Parties agree such additional terms shall be null and void). Only the provisions of this Agreement shall apply to the Participant and the Participant end-users for access to and use of the Database.

- 11.12 Order of Precedence.** Except as otherwise expressly provided herein, should there be any conflict between the terms of this Agreement and the BAA, the terms of this Agreement shall take precedence.
- 11.13 Survival.** Notwithstanding any expiration or earlier termination of this Agreement, those provisions which by their meaning are intended to survive termination, including, or in addition to the following provisions of this Agreement relating to the following matters, shall survive termination in accordance with their terms: (Indemnification), (Representations and Warranties; Limitations), (Liability Limitations), (Survival), (Definitions), (General Provisions) and Exhibit A (Business Associate Addendum), and Exhibit B (Client Authorization form). Termination of this Agreement by a Party shall not relieve the other Party hereto from any liability that at the time of termination already accrued to the other Party or which thereafter may accrue in respect of any act or omission of such Party prior to termination or any continuing obligation imposed by this Agreement or Applicable Law.
- 11.14 Reference to Days.** All references in this Agreement to "days" will, unless otherwise specified, mean calendar days. For purposes of this Agreement, the words "business day(s)" shall mean any day other than a Saturday, Sunday or holiday recognized by the State of California.
- 11.15 Authorized Agent Signature.** By signing this Agreement, the undersigned represents and warrants that he or she has received and read a copy of this Agreement, inclusive of attachments and exhibits, and that he or she is either (a) the Participant or, (b) if the Participant is an organization, an individual acting on the Participant's behalf who is authorized to sign and enter into this Agreement.
- 11.16 Counterpart Signatures and Facsimile Signatures.** This Agreement may be executed and delivered in counterparts, all of which taken together shall constitute one single agreement between the Parties. A facsimile



COMMUNITY
INFORMATION
EXCHANGE



ARXXXXX

PHASE I PILOT PARTICIPATION AGREEMENT

transmission of the executed signature page of this Agreement shall constitute due and proper execution and delivery of this Agreement.

EXHIBIT A BUSINESS ASSOCIATE ADDENDUM

See Attached

The attached BAA applies to the Parties only to the extent that a business associate relationship exists within the meaning of 45 CFR 160.103.

EXHIBIT A



HIPAA: BUSINESS ASSOCIATE ADDENDUM

This Business Associate Addendum (“**BAA**”) is entered into by and between the Public Health Institute, a California nonprofit public benefit 501(c)3 corporation, on behalf of its program Ventura County Community Information Exchange, with a principal place of business at 1950 Franklin Street, Suite 600, Oakland, CA 94612 (“**VCCIE**”), and [ENTER NAME], with a principal place of business at [ENTER ADDRESS] (“**Participant**”).

VCCIE and Participant are each a “Party” to this BAA and are collectively referred to as the “Parties.” Any extensions or renegotiations of this BAA shall be reviewed and signed by both Parties.

Recitals

WHEREAS, VCCIE and Participant have entered into an agreement(s) pursuant to which VCCIE provides to Participant certain services that now or in the future shall include, but not be limited to, the creation, receipt, maintenance, data analysis and/or transmission of protected health information for a function or activity regulated by HIPAA (“Services Agreement(s)”);

WHEREAS, to the extent that Participant is a “Covered Entity” (as defined by HIPAA), Participant is subject to the Administrative Simplification requirements of the Health Insurance Portability and Accountability Act (“HIPAA”) of 1996, Public Law 104-191, and regulations promulgated thereunder, including the Standards for Privacy of Individually Identifiable Health Information at 45 Code of Federal Regulations (C.F.R.) Parts 160 and Subparts A and E of 45 C.F.R. Part 164 (“Privacy Regulations”) and the Security Standards for Electronic Protected Health Information (“Security Regulations”) at 45 C.F.R. Parts 160 and Subparts A and C of 45 C.F.R. Part 164, as amended by the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) of 2009, Public Law 111-5, and regulations promulgated thereunder including the Breach Notification Regulations at Subpart D of 45 C.F.R. Part 164, and is subject to certain state privacy laws;

WHEREAS, to the extent that VCCIE is, on behalf of Participant, creating, receiving, maintaining, performing data analysis and/or transmitting protected health information for a function or activity regulated by HIPAA, VCCIE is a “Business Associate” (as defined by HIPAA) and is subject to certain provisions of HIPAA, and regulations promulgated thereunder, as required by the HITECH Act and regulations promulgated thereunder;

WHEREAS, to the extent Participant is not a “Covered Entity” (as defined by HIPAA), then VCCIE is the Covered Entity hereunder and Participant is the Business Associate, as Participant will be creating, receiving, maintaining, performing data analysis and/or transmitting protected health information for a function or activity regulated by HIPAA on behalf of VCCIE;

WHEREAS, Covered Entity and Business Associate are required to enter into a contract in order to mandate certain protections for the privacy and security of Protected Health Information;

NOW, THEREFORE, in consideration of the foregoing, of the promises set forth herein, and for other good and valuable consideration, the receipt and adequacy of which is hereby acknowledged, the parties agree as follows:

1. **Definitions.** All capitalized terms used in this BAA not specifically defined otherwise below or in the Services Agreement(s) shall have the same definitions as given to them under HIPAA.
 - 1.1. **Agreement** as used in this document means both this BAA and the Services Agreement(s) to which this BAA applies, as specified in such Services Agreement(s).
 - 1.2. **Breach** means, unless expressly excluded under 45 C.F.R. § 164.402, the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under Subpart E of 45 C.F.R. Part 164 which compromises the security or privacy of the Protected Health Information and as more particularly defined under 45 C.F.R. § 164.402.
 - 1.3. **Business associate** has the meaning given such term in 45 C.F.R. § 160.103.
 - 1.4. **Confidential information** refers to information not otherwise defined as Protected Health Information in Section 1.15 below, but to which state and/or federal privacy and/or security protections apply.
 - 1.5. **Data aggregation** has the meaning given such term in 45 C.F.R. § 164.501.
 - 1.6. **Designated record set** has the meaning given such term in 45 C.F.R. § 164.501.
 - 1.7. **Disclose** and **disclosure** mean the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
 - 1.8. **Electronic health record** has the meaning given such term in 42 U.S.C. § 17921.
 - 1.9. **Electronic media** means:
 - 1.9.1. Electronic storage material on which data is or may be recorded electronically including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
 - 1.9.2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.
 - 1.10. **Electronic protected health information** (“ePHI”) means individually identifiable health information that is transmitted by or maintained in electronic media.
 - 1.11. **Health care operations** has the meaning given such term in 45 C.F.R. § 164.501.
 - 1.12. **Individual** means the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

- 1.13. **Individually identifiable health information** means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or 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, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 C.F.R. § 160.103.
- 1.14. **Information system** means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
- 1.15. **Protected Health Information** as used in this Agreement and unless otherwise stated, refers to and includes both Protected Health Information as defined at 45 C.F.R. § 160.103 and personal information ("PI") as defined in the Information Practices Act at California Civil Code § 1798.3(a), except that as used herein, the term shall refer only to Protected Health Information that Business Associate creates, receives, maintains, or transmits on behalf of or from Covered Entity. Protected Health Information includes information in any form, including paper, oral, and electronic.
- 1.16. **Required by law** means a mandate contained in law that compels an entity to make a use or disclosure of Protected Health Information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing benefits.
- 1.17. **Secretary** means the Secretary of the U.S. Department of Health and Human Services or the Secretary's designee.
- 1.18. **Security incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- 1.19. **Services** has the same meaning as in the Services Agreement(s).
- 1.20. **Unsecured protected health information** means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under 42 U.S.C. § 17932(h)(2).
- 1.21. **Use** and **uses** mean, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information within the entity that maintains such information.

2. Obligations of Business Associate.

- 2.1. **Compliance with Regulatory Obligations of Business Associate.** Business Associate shall perform and comply with all the applicable obligations and requirements imposed upon business associates pursuant to HIPAA.
- 2.2. **Permitted Receipt, Use and Disclosure of Protected Health Information.** Business Associate may receive, Use and Disclose Protected Health Information to the minimum extent necessary to perform Business Associate's obligations, functions, activities and/or services under the Services Agreement(s), and as otherwise permitted or required by this BAA, the Services Agreement(s), or applicable law. Business Associate shall not Use or Disclose Protected Health Information in any manner that would violate the requirements of HIPAA if done by Covered Entity.
- 2.3. **Specified Permitted Uses of Protected Health Information.** Without limiting the generality of Section 2.2 (Permitted Use and Disclosure of Protected Health Information), Business Associate may Use Protected Health Information as follows:
 - 2.3.1. For the proper management and administration of Business Associate.
 - 2.3.2. To carry out the legal responsibilities of Business Associate.
 - 2.3.3. To provide Data Aggregation services relating to the Health Care Operations of Covered Entity or, if applicable, an organized health care arrangement of which the Covered Entity is a member of and to the extent provided by the Services Agreement(s) or other agreement.
 - 2.3.4. To perform services related to the creation of De-Identified Data.
- 2.4. **Specified Permitted Disclosures of Protected Health Information.** Without limiting the generality of Section 2.2 (Permitted Receipt, Use and Disclosure of Protected Health Information), Business Associate may Disclose Protected Health Information as follows:
 - 2.4.1. Pursuant to the direction of the Covered Entity;
 - 2.4.2. For the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate:
 - 2.4.2.1. If the disclosure is Required by Law; or
 - 2.4.2.2. If Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purposes for which it was Disclosed to the person, and if the person promptly notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached.
- 2.5. **Specified Permitted Receipt of Protected Health Information.** Without limiting the generality of Section 2.2 (Permitted Receipt, Use and Disclosure of Protected Health Information), and in

addition to Business Associate being permitted to disclose Protected Health Information to its Subcontractors subject to Section 2.12 below, Business Associate may receive Protected Health Information from another business associate of Covered Entity pursuant to the direction of the Covered Entity.

- 2.6. **Compliance with Other Applicable Law.** To the extent that other state and/or federal laws provide additional, stricter and/or more protective (collectively, “more protective”) privacy and/or security protections to Protected Health Information or other confidential information covered under this Agreement beyond those provided through HIPAA, Business Associate agrees:
- 2.6.1. To comply with the more protective of the privacy and security standards set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and
 - 2.6.2. To treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to Section 2.9 of this Agreement.
 - 2.6.3. Examples of laws that provide additional and/or stricter privacy protections to certain types of Protected Health Information and/or confidential information, as defined in Section 1 of this Agreement, include, but are not limited to the Information Practices Act, California Civil Code §§ 1798-1798.78, Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2, Welfare and Institutions Code § 5328, and California Health and Safety Code § 11845.5.
 - 2.6.4. If Business Associate is a Qualified Service Organization (“QSO”) as defined in 42 C.F.R. § 2.11, Business Associate agrees to be bound by and comply with subdivisions (2)(i) and (2)(ii) under the definition of QSO in 42 C.F.R. § 2.11.
- 2.7. **Prohibition on Sale of Protected Health Information; No Remuneration.** Business Associate shall not directly or indirectly receive remuneration in exchange for Protected Health Information, except with the prior written authorization of Covered Entity, and then, only as permitted by HIPAA and the HITECH Act. The term Protected Health Information, as used in this Section, only refers to Protected Health Information as defined in 45 C.F.R. § 160.103.
- 2.8. **Safeguards.** Business Associate shall Use appropriate safeguards and comply, where applicable, with 45 C.F.R. §§ 164.302 through 164.316 with respect to ePHI and will apply appropriate safeguards to prevent the Use or Disclosure of the Protected Health Information in any form, including electronic form other than as provided for by this BAA.
- 2.8.1. Business Associate shall use safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Protected Health Information and other confidential data and comply, where applicable, with Subpart C of 45 C.F.R. Part 164 with respect to ePHI, to prevent use or disclosure of the information other than as provided for by this Agreement. Such safeguards shall be, at a minimum, at Federal Information Processing Standards (FIPS) Publication 199 protection levels. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the

standards, implementation specifications and other requirements of Subpart C of 45 C.F.R. Part 164, in compliance with 45 C.F.R. § 164.316. Business Associate shall maintain a comprehensive written information privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities.

2.8.2. Business Associate shall, at a minimum, utilize an industry-recognized security framework when selecting and implementing its security controls, and shall maintain continuous compliance with its selected framework as it may be updated from time to time. Examples of industry-recognized security frameworks include but are not limited to:

2.8.2.1. NIST SP 800-53 - National Institute of Standards and Technology Special Publication 800-53

2.8.2.2. FedRAMP - Federal Risk and Authorization Management Program

2.8.2.3. PCI - PCI Security Standards Council

2.8.2.4. ISO/IEC 27002 - International Organization for Standardization / International Electrotechnical Commission standard 27002

2.8.2.5. IRS PUB 1075 - Internal Revenue Service Publication 1075

2.8.2.6. HITRUST CSF - HITRUST Common Security Framework

2.8.3. Business Associate shall maintain, at a minimum, the most current industry standards for transmission and storage of Protected Health Information and other confidential information. Without limiting the foregoing, Business Associate shall maintain, at a minimum, the most current industry standards, for encryption of all workstations, laptops, and removable media devices containing Protected Health Information and data transmissions of Protected Health Information, unless Business Associate complies with applicable requirements of the Security Regulations, including 45 C.F.R. §§ 164.306 and 164.312.

2.8.4. Business Associate shall apply security patches and upgrades, and keep virus software up-to-date, on all Business Associate systems on which Protected Health Information and other confidential information may be used.

2.8.5. Business Associate shall identify the security official who is responsible for the development and implementation of the policies and procedures required by 45 C.F.R. Part 164, Subpart C.

2.9. **Reporting Unauthorized Uses and Disclosures**. Business Associate shall implement reasonable systems for the discovery and prompt reporting of any Breach or Security Incident. Business Associate shall report to Covered Entity, without unreasonable delay, and in accordance with the deadlines provided below, any Use or Disclosure of Protected Health Information not permitted by this BAA of which Business Associate becomes aware, including any Use or Disclosure involving Protected Health Information and any Breach of Privacy or Security as defined in the

Terms and Conditions of the Services Agreement(s). Without limiting the generality of the foregoing:

2.9.1. Reporting of Breaches of Privacy or Security.

2.9.1.1. Following the discovery of (a) any access to, Use or Disclosure of Protected Health Information which is not permitted by the Services Agreement(s) (including any Breach of Privacy or Security) or (b) any Security Incident, Business Associate shall notify Covered Entity by contacting Covered Entity's designated privacy contact person without unreasonable delay, and in no case later than forty-eight (48) hours after discovery of the Breach of Privacy or Security or any Security Incident; provided, however, that the Parties acknowledge and agree that this Section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which notice to Covered Entity by Business Associate shall be required only upon request.

2.9.1.2. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, Use or Disclosure of Protected Health Information. Covered Entity will advise Business Associate of any subsequent changes to the privacy contact person's contact information.

2.9.2. **Required Actions.** Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, Use or Disclosure of Protected Health Information (collectively "Exposure"), the party responsible for, or otherwise experiencing, the Exposure, shall take:

2.9.2.1. Prompt action to mitigate any risks or damages involved with the Exposure;

2.9.2.2. Any action pertaining to such unauthorized disclosure required by applicable federal and state law; and

2.9.2.3. Any necessary corrective actions, at its own costs, reasonably required by Covered Entity in the context of an Exposure not within the scope of the applicable VCCIE Client Authorization Form, and commensurate with the extent to which an incident is attributable to the party responsible for, or otherwise experiencing, the Exposure, such as but not limited to conducting breach assessment and reporting, and providing identity theft protections and credit monitoring for affected individuals.

2.9.3. **Investigations.** The party responsible for, or otherwise experiencing, the Exposure shall immediately investigate such Exposure. Such party shall report the following to Covered Entity without unreasonable delay:

2.9.3.1. Exposure details including the date of the Exposure and when it was discovered;

- 2.9.3.2. The identification of each individual whose unsecured Protected Health Information has been, or is reasonably believed by such party to have been accessed, acquired, used or disclosed during the Exposure;
 - 2.9.3.3. The nature of the data elements involved and the extent of the data involved in the Exposure;
 - 2.9.3.4. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed Protected Health Information or confidential data;
 - 2.9.3.5. A description of where the Protected Health Information or confidential data is believed to have been improperly transmitted, sent, or utilized;
 - 2.9.3.6. A description of the probable causes of the improper use or disclosure;
 - 2.9.3.7. Any other available information that the Business Associate is required to include in notification to the individual under 45 C.F.R. § 164.404(c);
 - 2.9.3.8. Whether the Protected Health Information or confidential data that is the subject of the Exposure included Unsecured Protected Health Information;
 - 2.9.3.9. Whether a law enforcement official has requested a delay in notification of individuals whose data is the subject of the Exposure because such notification would impede a criminal investigation or damage national security and whether such notice is in writing; and
 - 2.9.3.10. Whether, to such party's reasonable knowledge, Section 13402 of the HITECH Act (codified at 42 U.S.C. § 17932), California Civil Code §§ 1798.29 or 1798.82, or any other federal or state laws requiring individual notifications of breaches are triggered.
- 2.9.4. **Complete Report.** The party responsible for, or otherwise experiencing, the Exposure shall provide a complete written report of the investigation ("Final Report") to the Covered Entity contact within seven (7) working days of the discovery of the security incident or breach. The party responsible for, or otherwise experiencing, the Exposure shall comply with Covered Entity's additional form and content requirements for reporting of such privacy incident.
- 2.9.4.1. The Final Report shall provide a comprehensive discussion of the matters identified in Section 2.9.3 above and the following:
 - 2.9.4.1.1. An assessment of all known factors relevant to a determination of whether a breach occurred under HIPAA and other applicable federal and state laws;
 - 2.9.4.1.2. A full, detailed corrective action plan, including its implementation date and information on mitigation measures taken to halt and/or contain the improper use or disclosure and to reduce the harmful effects of the breach;

2.9.4.1.3. The potential impacts of the incident, such as potential misuse of data, identity theft, etc.; and

2.9.4.1.4. A corrective action plan describing how the party responsible for, or otherwise experiencing, the Exposure will prevent reoccurrence of the incident in the future. Notwithstanding the foregoing, all corrective actions are subject to the approval of Covered Entity.

2.9.4.2. If Covered Entity requests additional information, the party responsible for, or otherwise experiencing, the Exposure shall make reasonable efforts to provide Covered Entity with such information. A supplemental written report may be used to submit revised or additional information after the Final Report is submitted.

2.9.4.3. Covered Entity will review and approve or disapprove the determination by the party responsible for, or otherwise experiencing, the Exposure regarding whether a breach occurred, whether the security incident or breach is reportable to the appropriate entities, if individual notifications are required, and the corrective action plan within seven (7) working days of receipt.

2.9.4.4. **New Submission Timeframe.** If the party responsible for, or otherwise experiencing, the Exposure does not complete a Final Report within the seven (7) working day timeframe specified in Section 2.9.4 above, such party shall request approval from Covered Entity within the seven (7) working day timeframe of a new submission timeframe for the Final Report. The Parties acknowledge that a new submission timeframe requires the approval of Covered Entity.

2.10. **Notification of Individuals.** To the extent individual notifications are required, then the party, or its agents, to which the breach is attributable, if promptly requested by Covered Entity in writing, shall notify individuals accordingly at such party's own expense, commensurate with the extent attributable to such party. The notifications shall comply with applicable federal and state law. All such notifications shall be coordinated with Covered Entity. Covered Entity shall approve the time, manner and content of any such notifications. The Parties acknowledge that such review and approval by Covered Entity must be obtained before the notifications are made.

2.11. **Reporting of Breaches to Entities Other Than Covered Entity.** If the cause of a breach of Protected Health Information is attributable to Business Associate or its subcontractors, Business Associate agrees that Covered Entity shall make all required reporting of the breach as required by applicable federal and state law, including any required notifications to media outlets, the Secretary, and other government agency/regulator; provided, however, such report or notification shall be provided to Business Associate to allow a reasonable opportunity to comment in advance of submission or other publication. Any fines associated with a breach attributable to Business Associate or its subcontractors shall be the responsibility of the party that caused the breach, commensurate with the extent attributable to such party. Such party shall also be responsible for the costs associated with providing credit monitoring for the subjects of such breach, commensurate with the extent attributable to such party and to the extent required by applicable law.

- 2.12. **Arrangements with Subcontractors**. Business Associate shall enter into a BAA with any Subcontractor of Business Associate that creates, receives, maintains, or transmits Protected Health Information on behalf of Business Associate, pursuant to which the Subcontractor shall agree to comply with the applicable requirements of HIPAA and the same (or more stringent) restrictions and conditions that apply to Business Associate with respect to that Protected Health Information pursuant to this BAA, and pursuant to which Business Associate shall obtain satisfactory assurances that the Subcontractor shall appropriately safeguard that Protected Health Information.
- 2.13. **Individuals' Access to Protected Health Information**. Business Associate shall make available Protected Health Information in a designated record set as necessary to satisfy the requirements of 45 C.F.R. § 164.524.
- 2.14. **Individuals' Request for Amendments to Protected Health Information**. Business Associate shall incorporate amendments to Protected Health Information as and to the extent required for compliance with 45 C.F.R. § 164.526.
- 2.15. **Individuals' Requests for Accountings of Disclosures**. Business Associate shall document Disclosures of Protected Health Information and provide information sufficient to respond to a request by a Patient for an Accounting of Disclosures in compliance with 45 C.F.R. § 164.528.
- 2.16. **Other Obligations**. To the extent that Business Associate is, pursuant to the Services Agreement(s) or this BAA, responsible to carry out an obligation of Covered Entity under HIPAA, Business Associate shall comply with the requirements of HIPAA that apply to Covered Entity in the performance of that obligation.
- 2.17. **Access to Practices, Facilities, Books and Records**. Business Associate shall make its internal practices, facilities, books, and records relating to the Use and Disclosure of Protected Health Information, available to Covered Entity, during normal business hours at mutually agreed upon times, and available to the Department of Health Care Services and the Secretary for purposes of determining Covered Entity's or Business Associate's compliance under HIPAA. Business Associate shall immediately notify Covered Entity of any requests made by DHCS or the Secretary and provide Covered Entity with copies of any documents produced in response to such request.
3. **Covered Entity's Obligations**.
- 3.1. **Notice of Change in Privacy Practices**. Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's Notice of Privacy Practices in accordance with 45 C.F.R. §164.520, to the extent that that limitation may affect Business Associate's Use or Disclosure of Protected Health Information, as soon as reasonably practicable, and in no case more than ten (10) business days after the change to the notice of privacy practices containing such limitation.
- 3.2. **Notice of Change in Permissions**. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an individual to Use or Disclose Protected Health Information, to the extent that that change may affect Business Associate's Use or Disclosure of Protected Health Information, as soon as reasonably practicable, and in no case more than ten (10) business days after the date when Covered Entity learns of the change in permissions. Business

Associate shall abide by each change in, or revocation of, permission described above in this clause (b).

- 3.3. **Notice of Change in Use.** 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 45 C.F.R. §164.522, to the extent that that restriction may affect Business Associate's Use or Disclosure of Protected Health Information, as soon as reasonably practicable, and in no case more than ten (10) business days after the date when Covered Entity learns of the restriction. Business Associate shall abide by each restriction described above in this clause (c).
- 3.4. **Notice of SSA Data.** Covered Entity shall provide advance notice to Business Associate before providing Business Associate with data that was verified by or provided by the Social Security Administration ("SSA data") and is subject to an agreement between DHCS and SSA.
- 3.5. **Appropriate Requests.** Covered Entity shall not request that Business Associate Use or Disclose Protected Health Information in any manner that would not be permissible under HIPAA if done by Covered Entity.

4. **Term and Termination.**

- 4.1. **Term.** Subject to the other provisions of this Section 4 (Term and Termination), the term of this BAA shall be coextensive with that of the Services Agreement(s).
- 4.2. **Breach Pattern of Practice.** If a party knows of a pattern of activity or practice by the other party that constitutes a material breach or violation of its obligations under HIPAA or this BAA, such party shall immediately notify the other party of that breach. If such other party is unsuccessful in curing that breach within a reasonable time period specified by the notifying party, the notifying party may terminate this BAA and the Services Agreement(s), if feasible, upon written notice to the other party.
- 4.3. **Conduct Upon Termination.** Upon termination or expiration of this BAA, Business Associate and Covered Entity acknowledge that return or destruction of Protected Health Information is not feasible. Accordingly, Business Associate shall extend the protections of this BAA, including Section 2.8 (Safeguards), to any Protected Health Information for so long as it is not destroyed, and limit further Uses and Disclosures of that Protected Health Information to those purposes that make the return or destruction not feasible, for as long as Business Associate or any Subcontractor of Business Associate maintains that Protected Health Information. Upon the expiration of this period of infeasibility, if any, Business Associate shall destroy all Protected Health Information that it has retained. If Protected Health Information is to be destroyed pursuant to this Section 4.3 (Conduct Upon Termination) or pursuant to the Services Agreement(s), Business Associate shall certify in writing to Covered Entity that the Protected Health Information has been destroyed.
- 4.4. **Data Destruction.** Data destruction methods for Protected Health Information or confidential information must conform to U.S. Department of Defense standards for data destruction DoD 5220.22-M (7 Pass) standard or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of Covered Entity for Protected Health Information, and of the disclosing party for

any confidential information.

- 4.5. **Destruction of Hard Copy Confidential Information.** Protected Health Information or confidential information in hard copy form must be disposed of through confidential means, such as crosscut shredding and pulverizing.
5. **Relationship to Services Agreement(s).** In the event that a provision of this BAA is contrary to a provision of the Services Agreement(s) pertaining to Business Associate's performance of its obligations as a business associate, the provisions of this BAA shall control.
6. **Cooperation in Investigations.** The Parties acknowledge that certain breaches or violations of this BAA may result in litigation or investigations pursued by federal or state governmental authorities of the United States resulting in civil liability or criminal penalties. Each Party shall cooperate in good faith in all respects with the other Party in connection with any request by a federal or state governmental authority for additional information and documents or any governmental investigation, complaint, action or other inquiry.
7. **Amendment.** The Parties agree to take that action from time to time as is necessary to amend this BAA for Covered Entity and Business Associate to comply with HIPAA or other applicable law. The Parties agree that this BAA may only be modified by mutual written amendment, signed by both Parties, effective on the date set forth in the amendment.
8. **Interpretation.** Any ambiguity in this BAA shall be interpreted to permit compliance with HIPAA.

Covered Entity and Business Associate have entered into this BAA and agree to the terms herein as of the Effective Date of the Services Agreement(s).

EXHIBIT B - CLIENT AUTHORIZATION FORM



CLIENT AUTHORIZATION FORM FOR THE USE AND DISCLOSURE OF PROTECTED HEALTH AND PERSONAL INFORMATION

Full Client Name:		Email:	
Date of Birth:		Intake Organization:	
Phone number¹:		Care Coordinator:	

1. Overview of the VCCIE Service.

The Ventura County Community Information Exchange ("VCCIE") provides access to a referral platform (a protected database accessible online by service providers) that allows social service providers an efficient tool for making referrals and providing care coordination on behalf of consented clients ("You"). In addition, the VCCIE allows clients to create client portals on the platform, providing them a view of their open referrals and service providers. These providers offer health, social, and community resource services ("Services"), described in more detail [here](https://venturacountycie.org/client-authorization-resources/) (https://venturacountycie.org/client-authorization-resources/).

2. Who Will Have Access to Your Information?

For the purposes of this document, Participants refers to those organizations who have signed an agreement with VCCIE that requires them to agree to protect Your Information entered into the database and only use it to provide You with Services.

Participants may include healthcare providers (like hospitals and doctors), health insurance providers (like managed care plans), community-based organizations (like those offering medically tailored meals or housing services), school-based providers (like school nurses or counselors), State and county agencies, or providers and case managers at correctional facilities. See [here](https://venturacountycie.org/client-authorization-resources/) (https://venturacountycie.org/client-authorization-resources/) for a list of Participants.

By signing this form, You authorize Participants to disclose the Information to Be Shared to the VCCIE. You also authorize VCCIE to use, store, and share your Information, as more fully described below, with Participants. Additionally, You authorize Participants to use, store, and share the Information.

3. What Information Will Be Shared?

You authorize that Your personal, financial, and health information ("Information") will be shared to provide You with the Services described above. Go online [here](https://venturacountycie.org/client-authorization-resources/) (https://venturacountycie.org/client-authorization-resources/) to see descriptions of the

¹Providing Your phone number is voluntary, and means You consent to receive texts or calls regarding Your consent choices and for referrals through the VCCIE (standard messaging and calling rates may apply).

EXHIBIT B - CLIENT AUTHORIZATION FORM

types of information to be shared. Information includes:

- All health information relating to Your medical history, condition and treatment received, except for sensitive health information that requires your specific authorization in Section 4 below
- Information related to the access to and provision of social and educational services (such as housing, food, literacy skills, and transportation)

4. Purpose of Sharing Information.

Your Information may be used by and shared with Participants and VCCIE for future treatment, payment, and health care operations, as well as for the purposes of providing You with health, social, and community resource services as described above. Your Information will be shared as permitted by the Health Insurance Portability and Accountability Act (“HIPAA”), the federal rules about Substance Use Disorder data (“Part 2 Rules”), or by this Authorization.

By checking the boxes, You specifically authorize sharing of the following information:

- ☐ Information from health care providers about my mental health diagnosis or treatment that is protected under Welfare and Institutions Code § 5328 (excluding psychotherapy notes) and Information from Substance Use Disorder (SUD) programs (includes SUD diagnoses and medications, inpatient stays and outpatient visits or residential treatment, provider names and contact information, and names of the treatment programs) that is protected under 42 C.F.R. Part 2 and/or State law _____(initial)
- ☐ Information about Your HIV test results _____(initial)
- ☐ Abortion, reproductive health, and/or gender affirming treatment information _____(initial)

The disclosures of SUD, reproductive health, or medical information on abortion / abortion-related services permitted by this Authorization **do not** include disclosures for civil, criminal, administrative, or legislative proceedings against You, the patient. Also, this Authorization does not permit sharing of medical information on abortion / abortion-related services with persons from out-of-state or federal law enforcement agencies.

5. Expiration or Cancellation of This Form.

This authorization will expire ten (10) years from the date of signature. You can cancel this Authorization at any time. Please see cancellation details [here](https://venturacountycie.org/client-authorization-resources/) (https://venturacountycie.org/client-authorization-resources/). Please allow a minimum of seven (7) business days to process. Your cancellation will take effect upon receipt, but Information shared based on Your past Authorization cannot be recalled or deleted.

EXHIBIT B - CLIENT AUTHORIZATION FORM

6. Your Rights.

- A. This authorization is voluntary, so You have the right to refuse signing it and You have the right to cancel this authorization.
- B. State and federal laws already allow organizations to share some of Your health information (including sensitive information) to treat You, obtain payment, and run their operations without Your consent. You understand that this Authorization does not change the information that can be shared under these laws. You understand that Your authorization is required to share Your SUD information, if applicable.
- C. If You decline to sign this authorization, doing so will not affect Your treatment or care, Your eligibility for Services or Your ability to receive them, or payment for Services. However, by not signing this Authorization, Participants and VCCIE may not be able to coordinate the Services You receive, and You may not be able to receive the full Services.
- D. The Information You authorize for release could be re-disclosed by Participants and shared in compliance with this Authorization and applicable laws and regulations. Such disclosure may no longer be protected by federal or State privacy and confidentiality laws.
- E. You have a right to inspect or receive a copy of Your authorization and/or the Information that is shared under this Authorization.

Client Signature: _____

Date: _____

If a Personal Representative* is signing on behalf of the Client, please sign below and state the Personal Representative's relationship to the Client:

Signature of Personal Representative: _____

Relationship to Client: _____

Date: _____

Name of Personal Representative (Printed): _____

*A Personal Representative is the person who has the authority, under California law, to make health care decisions on behalf of the patient and may include a parent or legal guardian, a person named in a written health care power of attorney or advanced directive, or a conservator.