Exhibit A

AGREEMENT BETWEEN COUNTY OF SONOMA AND THE CITY OF SANTA ROSA FOR MOBILE CRISIS RESPONSE PROGRAM FUNDING

This agreement (hereinafter "Agreement") dated on _____, 2025 (hereinafter "Effective Date") is by and between the County of Sonoma, a political subdivision of the State of California (hereinafter "County") and City of Santa Rosa (hereinafter "City").

RECITALS

WHEREAS, the California Department of Health Services has implemented a new Medi-Cal Mobile Crisis Benefit requiring counties to provide rapid response, individual assessment and community-based stabilization to Medi-Cal beneficiaries who are experiencing a behavioral health crisis beginning January 1, 2024;

WHEREAS, the Sonoma County Department of Health Services is partnering with the cities of Santa Rosa, Petaluma, Rohnert Park, Cotati, and Sonoma State University to expand their services in implementing this benefit through a regional collaboration approach;

WHEREAS, the Sonoma County Board of Supervisors allocated Measure O Sales Tax revenue in May 2023 to support the implementation of these city-level programs and participate in a collaborative evaluation of these programs along with the Department of Health Services' Mobile Support Team;

WHEREAS, the City of Santa Rosa's inRESPONSE mobile crisis response team is consistent with the requirements of the Medi-Cal Mobile Crisis benefit that utilizes behavioral health and emergency medical service teams to act as first responders to service calls that do not require law enforcement resources;

WHEREAS, the City of Santa Rosa is partnering with Buckelew Programs to operate inRESPONSE, to improve response to mental illness and substance abuse crises, and will operate teams of specially trained civilian first responders who respond to and proactively address calls for service that have traditionally (and unnecessarily) burdened law enforcement, emergency medical services and health care providers; and

WHEREAS, in the judgment of the Board of Supervisors, it is necessary and desirable to provide funding to the City of Santa Rosa as a one-time investment to assist in expanding the capabilities of their mobile support team program.

WHEREAS, County personnel provide clinical services for the City of Santa Rosa mobile support team, as described in Exhibit A ("inRESPONSE Services").

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

AGREEMENT

1. Contract Exhibits

This Agreement includes the following exhibits, which are hereby incorporated by reference as though fully set forth herein. In the event of a conflict between the terms in the body of this Agreement and any of the following exhibits, the terms in the body of this Agreement shall control.

Exhibit A. Scope of Work and Budget
Exhibit B. Insurance Requirements
Exhibit C. Special Terms and Conditions – Information Privacy & Security – HIPAA Business Associate Addendum

2. Funding Amount

County agrees to provide funding ("Program Funds") to City in the amount of $1,450,000 upon execution of this Agreement.

3. Use of Program Funds

City shall use Program Funds as described in Exhibit A (Scope of Work and Budget), attached hereto and incorporated herein by this reference (hereinafter "Exhibit A"). In the event City does not complete efforts as described in Exhibit A by the end of the term of this Agreement, City shall return to the County all unused Program Funds provided to City under this Agreement.

4. Documentation of Project

City shall provide a written report on the use of Program Funds, and any other reasonable information the County should request including data requested as part of the collaborative evaluation efforts, within ten days after the term end date of this Agreement.

5. Invoices

City agrees to provide County with invoices demonstrating City's expenditures under this Agreement with sufficient detail and frequency to reasonably demonstrate compliance with any County Measure O requirements.

All billing and payment invoices shall be submitted via email or to the following address:

Sonoma County Department of Health Services
Fiscal Department
Attention: Accounts Payable
1450 Neotomas Avenue, Suite 200
Santa Rosa, CA 95405

DHS.Fiscal@sonoma-county.org

6. Term and Termination

6.1. Term

The term of this Agreement shall be from July 1, 2024 to June 30, 2025.

6.2. Termination

Notwithstanding any other provision of this Agreement, at any time and without cause, County shall have the right, in its sole discretion, to terminate this Agreement by giving 5 days' advance written notice to City.

7. Publicity

Publicity generated by City for work performed or services offered or funded by this Agreement during the term of this Agreement and for one year following expiration of this Agreement shall make reference to the contribution of the County in making the project possible.

8. Non-Discrimination

City agrees to comply with applicable federal state and local laws prohibiting discrimination in employment or in the provision of services because of race, color, religion, national origin, age, sex, sexual orientation or mental or physical handicap or any other protected category. City agrees to comply with Sections 19-30 through 19-40 of the Sonoma County Code, prohibiting discrimination due to HIV infection or a related condition.

9. Indemnification

9.1. Funding

City agrees to accept all responsibility for loss or damage to any person or entity, including COUNTY, and to indemnify, hold harmless, and release COUNTY, its officers, agents, and employees, from and against any actions, claims, damages, liabilities, disabilities, or expenses, that may be asserted by any person or entity, including City, that arise out of, pertain to, or related to City's or its agents', employees', contractors', subcontractors', or invitees' activities relating to the funds provided under this Agreement. City's obligations under this Section apply whether or not there is concurrent negligence on County's part, but to the extent required by law, excluding liability due to County's conduct. County shall have the right to select its legal counsel at City's expense, subject to City's approval, which shall not be unreasonably withheld. This indemnification obligation is not limited in any way by any limitation on the amount or type of damages or compensation payable to or for City or its agents under workers' compensation acts, disability benefits acts, or other employee benefit acts.

8.2. Services

With regard to the inRESPONSE Services provided pursuant to this Agreement, each party shall indemnify, defend, protect, hold harmless, and release the other, its officers, agents, and employees, from and against any and all claims, loss, administrative proceedings, regulatory proceedings, damages, causes of action, liability, costs or expenses to the extent arising from or in connection with, or caused by any negligent act or omission, of such indemnifying party. This indemnification obligation shall not be limited in any way by any limitation on the amount or type of damages or compensation payable to or for the indemnifying party under workers' compensation acts, disability benefit acts, or other employee benefit acts.

10. Confidentiality

Contractor agrees to maintain the confidentiality of all patient medical records and client information in accordance with all applicable state and federal laws and regulations, including the requirement to implement reasonable and appropriate administrative, physical and technical safeguards to protect all confidential information. This Article 9 shall survive termination of this Agreement.

In addition, when subcontracting for provider services under this contract, Contractor must include all language from, "*Exhibit C. Special Terms and Conditions – Information Privacy & Security – HIPAA Business Associate Addendum*" in the provider sub-contract.

11. Compliance With Laws

City agrees to comply, and to ensure compliance by its employees, subcontractors, and agents with all applicable federal, state and local laws, regulations, and statutes and policies, applicable to the services provided under this Agreement as they exist now and as they are changed,

amended, or modified during the term of this Agreement. To the extent there is a conflict between federal or state law or regulation and a provision in this Agreement, City shall comply with the federal or state law or regulation. Noncompliance during the term of the Agreement will be considered a material breach and may result in termination of the Agreement or pursuit of other legal or administrative remedies.

12. Right to Audit and Inspect

City understands and agrees to permit County the right to audit and inspect all records, notes and writings of any kind to the extent permitted by law, for the purpose of monitoring City compliance with the terms and conditions of this Agreement.

13. Obligations after Termination

The following shall remain in full force and effect after termination of this Agreement: (1) Article 8, Non-Discrimination, (2) Article 9, Indemnification, and (3) Article **Error! Reference source not found.**, Confidentiality, (4) Article **Error! Reference source not found.**, Compliance With Laws.

14. No Political or Religious Activity

County funds shall be used only for the purposes specified in this Agreement and in any attachments thereto. No County funds shall be used for any political activity, or to further the election or defeat of any candidate for political office. No County funds shall be used for purposes of religious worship, instruction, or proselytizing.

15. Merger

This writing is intended both as the final expression of the Agreement between the parties hereto with respect to the included terms and as a complete and exclusive statement of the terms of the Agreement, pursuant to Code of Civil Procedure 1856. No modification of this Agreement shall be effective unless and until such modification is evidenced by a writing signed by both parties.

16. Severability

In the event that any provision of this Agreement shall be held by a court to be invalid or illegal for any reason, said invalidity or illegality shall not affect the remaining provisions of this Agreement.

17. Method and Place of Giving Notice

All notices shall be made in writing and may be given by personal delivery or by mail. Notices sent by mail should be addressed as follows:

To County:	To City:
Behavioral Health Director Behavioral Health Division Department of Health Services County of Sonoma 2227 Capricorn Way, Suite 207 Santa Rosa, CA 95407 707-565-4850	Pam Lorence Administrative Services Officer City of Santa Rosa 100 Santa Rosa Avenue, Room 10 Santa Rosa, CA 95404 707-543-3010 plorence@srcity.org

And when so addressed, shall be deemed given upon deposit in United States mail, postage prepaid. In all other instances, notices shall be deemed given at the time of actual delivery. Changes may be made in the names and addresses of the person to whom notices are to be given by giving notice pursuant to this paragraph.

18. Assignment/Delegation

Neither party shall assign, sublet, or transfer any interest in or delegate any duty under this Agreement without the written consent of the other, and no assignment shall have any force or effect whatsoever unless and until the other party shall have so consented.

19. Status of Parties

This Agreement shall not be construed to create a joint venture or partnership. Neither party is the agent of the other for any purpose. There are no third party beneficiaries to this Agreement, and it may be enforced only by the parties hereto.

20. Insurance

With respect to performance of work under this Agreement, City shall maintain and shall require all of its subcontractors, contractors, and other agents to maintain insurance as described in Exhibit B (Insurance Requirements), which is attached hereto and incorporated herein by this reference.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the Effective Date.

CITY OF SANTA ROSA:

Maraskeshia Smith, City Manager City of Santa Rosa	Dated

COUNTY OF SONOMA:
Approved; Certificate of Insurance on File with County:

Jennifer Solito, Interim Director Department of Health Services	Dated

Approved as to Substance:

Division Director or Designee	Dated

Approved as to Form:

Sonoma County Counsel	12-12-24 Dated

Approved as to Substance:

Sonya Rodriguez signed on behalf of Ken Tasseff Privacy & Security Officer or Designee	12/11/2024 Dated

Exhibit A. Scope of Work and Budget

Mobile Crisis Services Expansion

I. Program Description

A. inRESPONSE Expansion

1. Under this agreement, the City of Santa Rosa, will retain the services of Buckelew Programs to operate the inRESPONSE program to include mobile crisis services as defined by the California Department of Health Care Services (DHCS) Behavioral Health Information Notice No. 23-025 (BHIN 23-025) and specified by Sonoma County Behavioral Health (SCBH).
2. BHIN 23-025 establishes a new Medi-Cal Benefit for Mobile Crisis services providing rapid response, assessment, and stabilization to Individuals experiencing a mental health and/or substance use disorder (SUD) crisis ("behavioral health crisis"[1]).
3. All calls for service shall adhere to the guidelines outlined within this scope of work, regardless of the individual's Medi-Cal or insurance status.

II. Service Description

A. Mobile Crisis Services Benefit Overview

1. Mobile crisis services provide rapid response, individual assessment and community-based stabilization to Individuals who are experiencing a behavioral health crisis. Mobile crisis services are designed to provide relief to individuals experiencing a behavioral health crisis, including through de-escalation and stabilization techniques; reduce the immediate risk of danger and subsequent harm; and avoid unnecessary emergency department care, psychiatric inpatient hospitalizations, and law enforcement involvement. While mobile crisis services are intended to support an integrated approach to responding to both mental health and substance use related crises, and mobile crisis teams will be carrying, trained, and able to administer naloxone, this benefit is not intended to replace emergency medical services for medical emergencies.
2. Mobile crisis services include warm handoffs to appropriate settings and providers when the individual requires additional stabilization and/or treatment services; coordination with and referrals to appropriate health, social and other services and supports, as needed; and short-term follow-up support to help ensure the crisis is resolved and the individual is connected to ongoing care. Mobile crisis services are directed toward the individual in crisis but may include contact with a family member(s) or other significant support collateral(s) if the purpose of the collateral's participation is to assist the individual in addressing their behavioral health crisis and restoring the individual to the highest possible functional level. For children and youth,

[1] A "behavioral health crisis" refers to any event or situation associated with an actual or potential disruption of stability and safety as a result of behavioral health issues or conditions. A crisis may begin the moment things begin to fall apart (e.g., running out of psychotropic medications or being overwhelmed by the urge to use a substance they are trying to avoid) and may continue until the individual is stabilized and connected or re-connected to ongoing services and supports.

in particular, mobile crisis teams shall work extensively with parents, caretakers and guardians, as appropriate and in a manner that is consistent with all federal and state laws related to minor consent, privacy and confidentiality.

3. Mobile crisis services are provided by a multidisciplinary mobile crisis team at the location where the individual is experiencing the behavioral health crisis. Locations may include, but are not limited to, the individual's home, school, or workplace, on the street, or where an individual socializes.

B. Dispatch Requirements

1. Contractor shall establish a system for dispatching inRESPONSE and develop policies and procedures that shall include, but are not limited to:
   a. Identification of a single telephone number to serve as a crisis services hotline connected to the dispatch of mobile crisis teams to receive and triage individual calls;
   b. A standardized dispatch tool and procedures to determine when to dispatch a mobile crisis team;
   c. Procedures identifying how mobile crisis teams will respond to dispatch requests.
2. Crisis Services Hotline
   a. Contractor shall identify and post a single telephone number that Individuals who may require mobile crisis services can call. This number can be the same as the county's 24/7 access line, or an existing crisis line.
   b. Contractor shall coordinate with the 988 Suicide and Crisis Lifeline, local law enforcement and 911 systems, the Family Urgent Response System (FURS), and community partners to ensure individuals have information about mobile crisis services.
3. Standardized Dispatch Tool and Procedures
   a. Crisis services hotline operators shall use a standardized tool provided by SCBHC and set of procedures to determine when a mobile crisis team should be dispatched versus when an individual's needs can be addressed via alternative means (e.g., de-escalation by hotline operator, connection to other services, etc.). Contractor shall use the tool consistently to dispatch mobile crisis teams.
4. Response to Dispatch Requests
   a. Contractor shall have live staff to receive and respond to all calls from the mobile crisis services or received through the hotline. Contractor shall not use an answering service. If an individual has been screened either directly, or through an individual calling on their behalf to request assistance, and the standardized dispatch tool has been used to determine that the individual requires mobile crisis services, the contractor shall dispatch a team to respond to the individual. When it is dispatched, the mobile crisis team shall meet the individual who is experiencing the behavioral health crisis in the location where the crisis occurs, unless the individual requests to be met in an alternate location in the community or cannot be located.

C. Requirements for Initial Crisis Response

1. The initial mobile crisis response shall be provided at the individual's location or at an alternate location of the individual's choice in the community ("onsite") by a multidisciplinary mobile crisis team.
2. Mobile crisis teams shall meet the following standards:
    a. At least two providers listed in Appendix A shall be available for the duration of the initial mobile crisis response. It is a best practice for at least two providers to be physically present onsite, but contractors may allow one of the two required team members to participate via telehealth compliant with BHIN 23-018, only if the contractor determines that such an arrangement:
        i. Is necessary because it otherwise would result in a marked delay in a mobile crisis team's response time; and
    b. The use of such an arrangement poses no safety concerns for the individual or the single mobile crisis team member who is physically onsite during the initial mobile crisis response.
    c. At least one onsite mobile crisis team member shall be carrying, trained, and able to administer naloxone.
    d. At least one onsite mobile crisis team members shall be able to conduct a crisis assessment.
    e. The mobile crisis team providing the initial mobile crisis response shall include or have access to a Licensed Practitioner of the Healing Arts (LPHA) (see Appendix A) provided by SCBH. For example, a mobile crisis team could consist of one LPHA and one peer support specialist. It also could consist of two peer support specialists who have access to a LPHA via telehealth compliant with BHIN 23-018.
3. Use of Telehealth to Supplement Mobile Crisis Teams
    a. In addition to the staffing requirements listed above, mobile crisis teams may utilize telehealth to:
        i. Connect the individual with highly trained and specialized practitioners,
        ii. including psychiatrists and psychiatric nurse practitioners;
        iii. Connect the individual with a provider who can prescribe medications;
        iv. Deliver follow-up services;
        v. Consult with appropriate specialists for individuals who have intellectual and/or developmental disabilities (I/DD); and/or
        vi. Engage translators or interpreters for individuals who may need American Sign Language or other interpretation or translation services.
4. Role of Peer Support Specialists
    a. It is considered a national best practice to include individuals with lived experience as members of mobile crisis teams. A Peer Support Specialist may participate as a

mobile crisis team member if they have a current, State-approved Medi-Cal Peer Support Specialist certification, provide services under the direction of a Behavioral Health Professional, and meet all other mobile crisis services requirements, including required mobile crisis services training.

5. Role of Community Health Workers

    a. CMS has approved added Community Health Worker (CHW) services as a Medi-Cal benefit. CHWs may include individuals known by a variety of job titles, including promotors, community health representatives, navigators, and other non-licensed public health workers, including violence prevention professionals. A CHW that meets the minimum qualifications through the certificate pathway, or the work experience pathway as set forth in the California State Medicaid Plan and also completes required mobile crisis services training may provide mobile crisis services as part of the mobile crisis team.

6. Role of Emergency Medical Technicians, Paramedics, and Community Paramedics

    a. Emergency Medical Technicians (EMTs), Advanced Emergency Medical Technicians (AEMTs), Paramedics, and Community Paramedics that are licensed, certified, and/or accredited in accordance with applicable State of California requirements and who complete required mobile crisis services training may provide mobile crisis services as part of the mobile crisis team. EMTs, AEMTs, Paramedics and Community Paramedics may be best positioned to support physical examinations, when needed, and provide individualized care to individuals who are at risk of preventable hospital admission or re-admission due to chronic care or acute physical needs. These providers may also support a behavioral health professional's assessment to determine if an individual requires emergency transport to an alternative setting for continued care.

D. Mobile Crisis Service Encounter Requirements

1. Each mobile crisis services encounter shall include, at minimum:

    a. Initial face-to-face crisis assessment;

    b. Mobile crisis response;

    c. Crisis planning, as appropriate, or documentation in the individual's progress note of the rationale for not engaging the individual in crisis planning; and

    d. A follow-up check-in, or documentation in the individual's progress note that the individual could not be contacted for follow-up despite reasonably diligent efforts by the mobile crisis team.

2. When appropriate, each mobile crisis services encounter shall also include:

    a. Referrals to ongoing services; and/or

    b. Facilitation of a warm handoff.

    c. Contractor shall be able to deliver all mobile crisis service components, even though there may be some circumstances in which it is not necessary or appropriate to provide all components (e.g., if the mobile crisis team can de-

escalate a situation onsite, it may not be necessary to facilitate a warm handoff to a higher level of care).

3. Contractor shall not require prior authorization for the delivery of mobile crisis services. Consistent with the dispatch policies contractor may de-escalate and stabilize an individual via telephone and make a determination that mobile crisis services are not appropriate or necessary.
4. Initial Face-to-Face Crisis Assessment
    a. The mobile crisis team shall provide a brief, face-to-face crisis assessment to evaluate the current status of the individual experiencing the behavioral health crisis with the goal of mitigating any immediate risk of danger to self or others, determining a short-term strategy for restoring stability, and identifying follow-up care, as appropriate. The crisis assessment is distinct from a comprehensive SMHS or DMC/DMC-ODS assessment. If an individual is referred to SMHS and/or DMC/DMC-ODS services for further behavioral health treatment, the contractor shall ensure the individual receives a comprehensive SMHS or DMC/DMC-ODS assessment (as defined in BHIN23-068) when required.
    b. Any team member that has been trained to conduct a crisis assessment as part of required mobile crisis services training can deliver the initial face-to-face crisis assessment. When delivering a crisis assessment, mobile crisis teams shall use a standardized crisis assessment tool. As part of the training and technical assistance process, DHCS will develop a template that Medi-Cal behavioral health delivery systems may use as the standardized crisis assessment tool.
    c. Medi-Cal behavioral health delivery systems may also select or develop their own standardized tool, subject to DHCS approval during the implementation process.
    d. Medi-Cal behavioral health delivery systems shall ensure that the crisis assessment tool is responsive to youth and adult individuals from culturally diverse backgrounds, including but not limited to tribal communities, LGBTQ+ youth and adults, individuals with limited English proficiencies and individuals with disabilities, including co-morbid disabilities, I/DD, serious mental illness, traumatic brain injury, and individuals who are deaf or hard of hearing.
5. Mobile Crisis Response
    a. During the mobile crisis services encounter, contractor shall intervene to de-escalate the behavioral health crisis and stabilize the individual at the location where the crisis occurs, unless the individual requests to be met in an alternate location in the community.
    b. The mobile crisis response may include, but is not limited to:
        i. Trauma-informed on-site intervention for immediate de-escalation of behavioral health crises;
        ii. Skill development, psychosocial education and initial identification of resources needed to stabilize the individual;

iii. Immediate coordination with other providers involved in the individual's care;

iv. Immediate coordination with other crisis receiving and stabilization facilities (e.g., sobering centers, crisis respite, crisis stabilization units, psychiatric health facilities, psychiatric inpatient hospitals, general acute care hospitals, crisis residential treatment programs, etc.); and

v. Provision of harm reduction interventions, including the administration of naloxone to reverse an opioid overdose, as needed.

6. Crisis Planning

a. As appropriate during the mobile crisis services encounter, the mobile crisis team shall engage the individual and their significant support collateral(s), if appropriate, in a crisis planning process to avert future crises. Crisis planning may include:

i. Identifying conditions and factors that contribute to a crisis;

ii. Reviewing alternative ways of responding to such conditions and factors; and

iii. Identifying steps that the individual and their significant support collateral(s) can take to avert or address a crisis.

b. When appropriate, crisis planning may include the development of a written crisis safety plan. Contractor shall utilize a DHCS as the standardized tool for writing a crisis safety plan. Medi-Cal behavioral health delivery systems may also select or develop their own standardized tool, subject to DHCS approval during the implementation process.

c. To the extent information is available and appropriate, the written crisis safety plan shall include, but is not limited to:

i. A review of any immediate threats to the individual's or others' safety and well-being, such as accessible firearms or medications which could be used in a plan for self-harm or harm to others;

ii. Conditions and factors that contribute to a crisis;

iii. Alternative ways of responding to such conditions and factors;

iv. Additional skill development and psychosocial education;

v. A psychiatric advanced directive;

vi. Short and long-term prevention and strategies and resources the individual can use to avert or address a future crisis, including harm reduction strategies.

d. A copy of the crisis safety plan, if one is developed, shall be documented in the individual's clinical record, and provided to the individual and to their significant support collateral(s) if it is feasible and would benefit the individual's treatment.

e. The contractor shall note in the individual's progress notes if crisis planning was appropriate and if the individual was or was not able to engage in crisis planning.

The contractor may continue crisis planning and create or update a written crisis safety plan with the individual as part of follow-up check-ins.

7. Facilitation of a Warm Handoff
    a. In some cases, the individual may need to be transported to a higher level of care, such as a sobering center, crisis respite, crisis stabilization unit, psychiatric health facility (PHF), psychiatric inpatient hospital, general acute care hospital, or crisis residential treatment program. If the individual requires further treatment at a higher level of care, the contractor shall connect the individual with the appropriate care option by facilitating a warm handoff. The contractor shall also arrange for or provide transportation to effectuate the warm handoff, if needed.
8. Referrals to Ongoing Services
    a. Contractor shall refer individuals, as appropriate, to available ongoing mental health and/or SUD treatment, community- based supports, social services, and/or other supports to help mitigate the risk of future crises. Contractors shall identify appropriate services and make referrals or appointments during the initial mobile crisis response if appropriate, or as part of follow-up check-ins, as needed.
    b. Referral sources may include, but are not limited to:
        i. Primary care providers;
        ii. Outpatient behavioral health treatment providers, including providers that may offer further support with care coordination/case management;
        iii. Prescribers for mental health or SUD medications;
        iv. Indian Health Care Providers;
        v. Providers serving individuals with disabilities, including individuals with I/DD, including but not limited to Regional Centers;
        vi. Programs offering Intensive Care Coordination (ICC), Intensive Home-Based Services (IHBS), and Therapeutic Foster Care (TFC) services;
        vii. Crisis receiving and stabilization facilities (e.g., sobering centers, crisis respite, crisis stabilization units, psychiatric health facilities, psychiatric inpatient hospitals, general acute care hospitals, crisis residential treatment programs, etc.);

            Community support and mutual aid groups (e.g., National Alliance on Mental Illness, Alcoholics Anonymous, Narcotics Anonymous, SMART Recovery);
        viii. Care coordination supports identified by the individual's Managed Care Plan (MCP) or other sources (e.g., Enhanced Care Management (ECM) services); and
        ix. Other housing and community supports for assistance with obtaining housing, utility, and rent (e.g., housing shelters and providers to facilitate coordinated entry, places of worship, food pantries, soup kitchens, recreation centers, community centers).

c. Contractor shall document all referrals in the individual's progress note. Contractor shall coordinate with other providers serving the individual in crisis when appropriate

9. Follow-up Check-Ins

a. Contractor shall ensure that individuals receive a follow-up check-in within 72 hours of the initial mobile crisis response. The purpose of the follow-up check-in is to support continued resolution of the crisis, as appropriate, and should include the creation of or updates to the individual's crisis safety plan, or additional referrals to ongoing supports, as needed. If the individual received a referral to ongoing supports during the initial mobile crisis response, as part of follow-up the contractor shall check on the status of appointments and continue to support scheduling, arrange for transportation, and provide reminders as needed.

b. Follow-up may be conducted by any contractor mobile crisis team member who meets DHCS' core training requirements and may be conducted in-person or via telehealth consistent with BHIN 23-018. Follow-up may be conducted by a contractor mobile crisis team member that did not participate in the initial mobile crisis response. If the contractor mobile crisis team member conducting follow-up is not part of the mobile crisis team that provided the initial crisis response, the individual providing follow-up shall coordinate with the team members that participated in the initial mobile crisis response to gather information on the recent crisis and any other relevant information about the individual. There may be times when the contractor is unable to engage the individual in follow-up. Examples include but are not limited to the individual is in inpatient treatment, otherwise incapacitated, unwilling to engage, or cannot be reached despite reasonably diligent efforts. The contractor shall document those instances where the individual cannot be engaged for follow-up.

10. Documentation

a. Contractor shall document problems identified during the mobile crisis services encounter on the individual's problem list within the individual's medical record, consistent with documentation requirements outlined in BHIN 23-068 (or superseding guidance). In addition, contractor shall create a progress note that describes all service components delivered to the individual, including any follow-up check-ins, referrals to ongoing supports, crisis planning, or facilitation of a warm handoff made as part of the mobile crisis services encounter.

b. Contractor shall perform all documentation is the electronic health record system SmartCare.

11. Coordination with Other Delivery Systems

a. A mobile crisis response is a powerful indicator that an individual needs additional services or that something is not working well with their current array of services; it warrants an alert to other providers who are involved in the individual's care and coordinated follow-up.

b. Contractor shall establish policies and procedures to ensure mobile crisis services are integrated into a whole person approach to care. Policies and procedures may include, but are not limited to:

    i. Contractor shall alert an individual's Medi-Cal behavioral health delivery system within 48 hours of a mobile crisis response and provide basic information about the encounter (e.g., disposition of the mobile crisis call);

    ii. The Medi-Cal behavioral health delivery system shall inform the contractor if they are aware if the individual is receiving care management through targeted case management, ICC, ECM, or any other benefit including non-Medi-Cal benefits such as Full-Service Partnership;

    iii. The Medi-Cal behavioral health delivery system shall alert the individual's MCP, if known, of the behavioral health crisis; and

    iv. If a contractor receives information that an individual is receiving services from a care manager, it shall alert the individual's care manager(s) of the behavioral health crisis, as applicable, and coordinate referrals and follow-up consistent with privacy and confidentiality requirements.

c. Contractors shall ensure that they have the individual's consent for these disclosures in cases where consent is required by applicable law.

12. Service Setting Restrictions

a. With the exception of the settings listed in the next paragraph, the initial mobile crisis response shall be provided where the individual is in crisis, or at an alternate location of the individual's choosing. Examples of settings include, but are not limited to: Houses and multi-unit housing;

    i. Workplaces;
    ii. Public libraries;
    iii. Parks;
    iv. Schools;
    v. Homeless shelters;
    vi. Outpatient clinics;
    vii. Assisted living facilities; and
    viii. Primary care provider settings.

b. Mobile crisis services shall not be provided in the following settings due to restrictions in federal law and/or because these facilities and settings are already required to provide other crisis services:

    i. Inpatient Hospital;

    ii. Inpatient Psychiatric Hospital;

    iii. Emergency Department;

    iv. Residential SUD treatment and withdrawal management facility;

    v. Mental Health Rehabilitation Center;

vi. Psychiatric Health Facility;

vii. Special Treatment Program;

viii. Skilled Nursing Facility;

ix. Intermediate Care Facility;

x. Settings subject to the inmate exclusion such as jails, prisons, and juvenile detention facilities;

xi. Other crisis stabilization and receiving facilities (e.g., sobering centers, crisis respite, crisis stabilization units, psychiatric health facilities, psychiatric inpatient hospitals, crisis residential treatment programs, etc.).

E. Standards

1. Hours of Operation
   a. The program operates 24 hours/day; seven days/week; 365 days/year.
2. Certifications.
   a. Contractor shall acquire and maintain Medi-Cal Site Certification.
3. Response Times
   a. Mobile crisis teams shall arrive at the community-based location where a crisis occurs in a timely manner. Specifically, mobile crisis teams shall arrive:
      i. Within 60 minutes of the individual being determined to require mobile crisis services in urban areas; and
      ii. Within 120 minutes of the individual being determined to require mobile crisis services in rural areas.
   b. Timeliness standards are not included in network adequacy requirements or certification. DHCS will provide ongoing technical assistance to Medi-Cal behavioral health delivery systems to review response times and adjust timeliness standards, as needed.
4. Community Partnerships
   a. Medi-Cal behavioral health delivery systems shall maintain relationships with key community partners to support community engagement with mobile crisis services, coordination, and system navigation. Medi-Cal behavioral health delivery systems shall ensure that:
      i. Community partners are aware of the availability of mobile crisis services as a community resource; and
   b. Community partners understand how to request mobile crisis services to assist individuals experiencing behavioral health crises.
   c. Community partners may include, but are not limited to:
      i. Medical and behavioral health providers;
      ii. Primary care providers (including pediatric providers for children);

iii. Social services providers;

iv. Community health centers;

v. Federally qualified health centers;

vi. Indian health care providers;

vii. Crisis receiving and stabilization facilities (e.g., sobering centers, crisis respite, crisis stabilization units, psychiatric health facilities, psychiatric inpatient hospitals, crisis residential treatment programs, etc.);

viii. Hospitals;

ix. Schools;

x. Regional Centers;

xi. MCPs;

xii. Local courts;

xiii. Local departments of social services; and

xiv. Law enforcement.

d. As part of their implementation plans, Medi-Cal behavioral health delivery systems shall describe how they will ensure mobile crisis teams establish community partnerships and engage community partners in sharing information and conducting outreach about the availability of mobile crisis services for Individuals and how to request dispatch of a mobile crisis team for Medi-Cal individuals.

5. Law Enforcement

a. When a mobile crisis team is dispatched, it is considered a national best practice for the team to respond without law enforcement accompaniment unless special safety concerns warrant inclusion. When not required for safety reasons, law enforcement involvement in a behavioral health crisis can lead to an increase in unnecessary arrests and incarceration of individuals living with acute behavioral health needs.

b. Contractor shall coordinate with law enforcement and share information with law enforcement officers about how to request or coordinate mobile crisis dispatch, when appropriate. Contractor shall also work with law enforcement to determine how mobile crisis teams and law enforcement can best work together to safely resolve and de-escalate behavioral health crises, minimizing the role of law enforcement except when necessary and appropriate for safety reasons. As part of their implementation plans, contractor shall describe strategies to avoid unnecessary law enforcement involvement in mobile crisis services and describe how they will ensure mobile crisis teams coordinate with law enforcement to safely resolve and de-escalate crises.

c. While law enforcement officers may accompany a mobile crisis team when necessary for safety reasons, they shall not qualify as a member of the mobile crisis team for purposes of meeting Mobile Crisis Team Requirements. Similarly, Crisis Intervention Teams (CIT), which include specially trained law enforcement officers

who have undergone designated CIT training may not provide or be reimbursed for mobile crisis services, unless they meet the mobile crisis team requirements.

6. Transportation
    a. When needed, a mobile crisis team shall arrange for or provide transportation to an appropriate level of care or treatment setting. The mobile crisis team may transport the individual directly as part of providing the mobile crisis service. If the mobile crisis team cannot provide transportation itself, or if there are outstanding medical or safety concerns, the mobile crisis team shall coordinate with non-medical transportation (NMT) providers, EMS, or law enforcement, if necessary, to arrange transportation and ensure the individual is connected with appropriate care. If EMS, NMT, or law enforcement is utilized to transport the individual directly to a higher level of care, the mobile crisis team shall remain onsite until the transportation provider arrives. At its discretion, the mobile crisis team may have one or more team members accompany the individual inside the vehicle to the higher level of care.
7. Cultural Competency, Linguistic Appropriate Care and Accessibility
    a. Medi-Cal behavioral health delivery systems shall comply with all applicable cultural competence and linguistic requirements in state and federal law, including those in Welfare and Institutions Code §4684(a)(9); California Code of Regulations, Title 9, §810.410; and BHIN 20-070.
8. Privacy and Confidentiality
    a. Contractor shall maintain the privacy and confidentiality of their patient's information in accordance with federal and state law. Mobile crisis teams typically will be health care providers subject to the privacy and security rules under the Health Insurance Portability and Accountability Act (HIPAA). While contractor and Medi-Cal behavioral health delivery systems will often be able to exchange protected health information in compliance with HIPAA, Medi-Cal behavioral health delivery systems shall be aware of HIPAA requirements that may limit mobile crisis teams' ability to share such information, such as HIPAA's minimum necessary requirement.
    b. In addition, there may be circumstances where mobile crisis teams are subject to the federal substance use disorder confidentiality regulation, 42 C.F.R. Part 2. Medi-Cal behavioral health delivery systems shall inquire whether any of their mobile crisis teams are subject to 42 C.F.R. Part 2 and, if so, ensure that workflows are in place to ask individuals for their consent when appropriate.
    c. If the individual is being served through a CalAIM initiative, some additional data sharing is permissible that might otherwise have been restricted under California law.
9. Other Considerations
    a. Children and Youth

i. Contractor shall respond to individuals of all ages, including children and youth experiencing behavioral health crises. Through crisis de-escalation and resolution, mobile crisis teams may help children, youth and their families avoid hospitalization and emergency out-of-home placements in many circumstances. For some children and youth, accessing crisis services may be their first introduction to the state's behavioral health system, making it a critical moment for early identification of mental health conditions and engagement into treatment.

ii. As part of required training, contractor shall participate in training on strategies to work effectively with children, youth and young adults experiencing behavioral health crises. Training may include, but is not limited to, delivering culturally responsive care, particularly when working with children, youth and young adults who are LGBTQ+, Black, Indigenous, and People of Color, involved in the child welfare system, or living with I/DD. In addition, mobile crisis teams shall abide by all state and federal minor consent laws. Required training shall also include an overview of existing minor consent obligations and appropriate protocols for communicating with parents, guardians and other responsible adults who may or may not be present at the time of the crisis.

iii. As part of their implementation plans, contractor shall describe how mobile crisis teams will coordinate with the FURS, Regional Centers, and other dispatch lines to ensure the most appropriate systems are responding to a crisis. contractor shall also describe how mobile crisis services providers will collaborate with and conduct outreach to schools (e.g., attending school health fairs to provide information on mobile crisis services, serving as a resource for school counselors and resource officers, etc.).

b. Tribal Communities

i. Contractor shall make a good faith effort to identify if the individual is a Tribal member, has seen an Indian Health Care Provider (IHCP) in the previous 12 months, or has a preference to receive follow-up care from an IHCP. Contractor may check with the individual or their significant support collateral(s), if appropriate; the individual's MCP; or the local IHCP to determine if the individual is a current IHCP patient or prefers to receive follow-up care from an IHCP. If the individual is an IHCP patient or prefers to be seen by an IHCP for follow-up care, the mobile crisis team shall make a good faith effort to connect the individual with the IHCP where they are a current patient or an IHCP that provides Medi-Cal-covered behavioral health services for follow-up care. If the individual sees a non-IHCP for follow-up care, the mobile crisis team shall make a good faith effort to share follow-up care information with the individual's IHCP, provided the mobile crisis team has the individual's consent to make such disclosure when required by applicable law.

c. Individuals with Intellectual and/or Developmental Disabilities

i. Individuals experiencing behavioral health crises may have co-occurring needs which require additional considerations in the provision of mobile crisis services. People with I/DD and co-occurring mental health conditions may experience sensory or communication challenges that may complicate de-escalation of a behavioral health crisis. Mobile crisis teams responding to an individual with I/DD shall ensure that natural supports (e.g., familial caregivers, personal attendants) are involved and consulted in the crisis response, if appropriate. To the extent possible, mobile crisis teams are encouraged to include a team member with I/DD expertise or have access to an individual with I/DD expertise (e.g., a Board-Certified Behavioral Analyst) via telehealth, which includes both synchronous audio-only (e.g., telephone) and video interactions.

ii. All members of mobile crisis teams shall participate in training on crisis response for individuals with I/DD, which may include, but is not limited to general characteristics of people with intellectual disability and autism spectrum disorder, co-occurrence of I/DD and mental health conditions, and crisis intervention strategies for serving this population (e.g., communication tactics and techniques, strategies to involve caregivers, etc.).

iii. Additionally, county mental health agencies are currently required to develop MOUs with Regional Centers to coordinate services, identify dually diagnosed individuals, and develop procedures for Regional Center staff and county mental health staff to collaborate in responding to individuals with co-occurring I/DD and mental health conditions.

iv. Contractor shall describe how their mobile crisis teams will meet the needs of individuals with I/DD who are experiencing behavioral health crises. Contractor is encouraged to conduct outreach to Regional Centers to promote communication and collaboration (e.g., provision of trainings for county mobile crisis teams, direction of people with I/DD in immediate crisis who contact regional center warmlines to county mobile crisis teams for support). Contractor is also encouraged to also seek supplementary training from local regional centers and/or the State Council on Developmental Disabilities.

10. Reporting

a. Contractor shall provide demographic, process, and outcomes data to SCBH on a periodic basis. SCBH will use this information to monitor and oversee contractor's implementation of the mobile crisis services benefit.

b. Contractor shall provide SCBH with data about each mobile crisis services encounter. The data shall include, but are not limited to:

i. Individual demographics (e.g., age, race, ethnicity, sexual orientation, and gender identity, etc.);

ii. Crisis location;

iii. Response times;

iv. Disposition of encounter (e.g., de-escalated in community-based setting, transported to crisis stabilization unit, etc.);

v. Professional titles of each team member participating in the mobile crisis response;

vi. Use of telehealth;

vii. If transportation was needed, and if so, what type of transportation was provided;

viii. Law enforcement involvement; and

ix. Information about follow-up check-ins.

c. Contractor shall conduct individual satisfaction surveys and follow additional DHCS guidance on data metrics, reporting processes and methods, and reporting frequency.

11. Training

a. Contractor shall ensure staff complete all of the following DHCS trainings:

i. Required Core Trainings

1. Crisis Intervention and De-escalation Strategies
2. Harm Reduction Strategies
3. Delivering Trauma-Informed Care
4. Conducting a Crisis Assessment
5. Crisis Safety Plan Development

ii. Required Enhanced Trainings

1. Crisis Response Strategies for Special Populations (may be a two-part training)
2. Children, Youth and Families
3. Tribal Communities
4. Individuals with Intellectual and Developmental Disabilities (I/DD)
5. Co-occurring Disorders/Responding to SUD Crises
6. Delivering Culturally Responsive Crisis Care

b. Other trainings as required by SCBH.

c. Contractor shall maintain records of completed trainings and provide those records to SCBH quarterly or upon demand.

d. Contractor shall provide a representative to all countywide Mobile Crisis Collaboration meetings.

F. Sonoma County Behavioral Health Provisions

1. SCBH shall provide contractor with the following:
   a. Access to electronic health record system SmartCare administered by SCBH.
   b. Trainings in Medi-Call documentation standards.
   c. DHS will provide LPHA staffing sufficient to meet the standards outlined in this contract.

III. Budget

	FTE	Amount ($)
Direct Personnel		
Paramedics for inResponse Van	6.0	472,215
Buckelew Staffing - contract for direct services		125,570
Fire Captain		190,000
Total Direct Personnel		787,785
Total Staff Benefits - 100% of staff salary (Paramedics and Fire Captain)		662,215
Total Personnel Costs		1,450,000
Operating Expenses		0
Total Operating Expenses		0
Total Indirect Expenses		0
Total Costs		1,450,000

Exhibit B. Insurance Requirements

City shall maintain insurance as described below unless such insurance has been expressly waived by the attachment of a **Waiver of Insurance Requirements**. The insurance shall be maintained for 1 year after all Program Funds have been disbursed. County understands and agrees that the City is self-insured. County agrees that City's self-insurance program satisfies the requirements set forth in this Exhibit B.

County reserves the right to review any and all of the required insurance policies and/or endorsements, but has no obligation to do so. Failure to demand evidence of full compliance with the insurance requirements set forth in this Agreement or failure to identify any insurance deficiency shall not relieve City from, nor be construed or deemed a waiver of, its obligation to maintain the required insurance at all times during the performance of this Agreement.

1. Workers Compensation and Employer's Liability Insurance

   a. Workers Compensation insurance with statutory limits as required by the Labor Code of the State of California.
   b. Employer's Liability with minimum limits of $1,000,000 per Accident; $1,000,000 Disease per employee; $1,000,000 Disease per policy.
   c. Required Evidence of Insurance: Certificate of Insurance.

2. General Liability Insurance

   a. Commercial General Liability Insurance on a standard occurrence form, no less broad than Insurance Services Office (ISO) Form CG 00 01.
   b. Minimum Limits: $1,000,000 per Occurrence; $2,000,000 General Aggregate; $2,000,000 Products/Completed Operations Aggregate. The required limits may be provided by a combination of General Liability Insurance and Commercial Umbrella Liability Insurance. If City maintains higher limits than the specified minimum limits, County requires and shall be entitled to coverage for the higher limits maintained by City.
   c. Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured retention exceeds $25,000, it must be approved in advance by County. City is responsible for any deductible or self-insured retention and shall fund it upon County's written request, regardless of whether City has a claim against the insurance or is named as a party in any action involving the County.
   d. **"County of Sonoma, its Officers, Agents, and Employees"** shall be additional insureds for liability arising out of City's ongoing operations. (ISO Endorsement CG 20 26 or equivalent).
   e. The insurance provided to the additional insureds shall be primary to, and non-contributory with, any insurance or self-insurance program maintained by them.
   f. The policy definition of "insured contract" shall include assumptions of liability arising out of both ongoing operations and the products-completed operations hazard (broad form contractual liability coverage, including the "f" definition of insured contract in ISO Form CG 00 01 or equivalent).
   g. The policy shall cover inter-insured suits between County and City and include a "separation of insureds" or "severability" clause which treats each insured separately.
   h. Required Evidence of Insurance
      i. Copy of the additional-insured endorsement or policy language granting additional-insured status; and

ii. Certificate of Insurance.

3. Automobile Liability Insurance

a. Minimum Limits: $1,000,000 combined single limit per accident.
b. Insurance shall apply to all owned vehicles if City owns vehicles.
c. Insurance shall apply to hired and non-owned vehicles.
d. Required Evidence of Insurance: Certificate of Insurance.

4. Professional Liability/Errors and Omissions Insurance

a. Minimum Limit: $1,000,000 per claim or per occurrence.
b. Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured retention exceeds $25,000, it must be approved in advance by County.
c. If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.
d. Required Evidence of Insurance: Certificate of Insurance.

5. Standards for Insurance Companies

Insurers, other than the California State Compensation Insurance Fund, shall have an A.M. Best's rating of at least A:VII.

6. Documentation

a. All required Evidence of Insurance shall be submitted prior to the execution of this Agreement. City agrees to maintain current Evidence of Insurance on file with County for the required period of insurance.
b. The name and address for Additional Insured endorsements and Certificates of Insurance is:

County of Sonoma - Department of Health Services
Attn: Contract and Board Item Development Unit
1450 Neotomas Avenue, Suite 200
Santa Rosa, CA 95405
DHS-Contracting@sonoma-county.org

c. Required Evidence of Insurance shall be submitted for any renewal or replacement of a policy that already exists at least 10 days before expiration or other termination of the existing policy.
d. City shall provide immediate written notice if: (1) any of the required insurance policies is terminated; (2) the limits of any of the required policies are reduced; or (3) the deductible or self-insured retention is increased.
e. Upon written request, certified copies of required insurance policies must be provided within 30 days.

7. Policy Obligations

City's indemnity and other obligations shall not be limited by the foregoing insurance requirements.

Exhibit C. Special Terms and Conditions – Information Privacy & Security – HIPAA Business Associate Addendum

This Business Associate Addendum ("Addendum") supplements and is made a part of the services agreement ("Agreement") by and between County of Sonoma ("County") and City of Santa Rosa ("Business Associate").

R E C I T A L S

WHEREAS, County is a Hybrid Entity as defined under 45 Code of Federal Regulations ("CFR") Section 164.103;

WHEREAS, City of Santa Rosa is a Business Associate as defined under 45 CFR Section 160.103;

WHEREAS, County wishes to disclose certain information to Business Associate pursuant to the terms of Addendum, some of which information may constitute Protected Health Information ("PHI"), including electronic Protected Health Information ("ePHI");

WHEREAS, County and Business Associate intend to protect the privacy and provide for the security of PHI, including ePHI, disclosed to Business Associate pursuant to Addendum in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104 191 ("HIPAA"), regulations promulgated thereunder by the U.S. Department of Health and Human Services, and other applicable laws; and

WHEREAS, as part of the HIPAA Regulations, the Privacy Rule and Security Rule require County to enter into a contract containing specific requirements with Business Associate prior to the disclosure of PHI, including ePHI, as set forth in, but not limited to, 45 CFR Sections 164.502(e), 164.504(e), and 164.308(b)(1) and contained in Addendum.

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

Part I: HIPAA Business Associate Addendum (Applies to HIPAA Business Associates)

1. Definitions

Terms used, but not otherwise defined, in Addendum shall have the same meaning as those terms in the HIPAA Regulations as set forth at 45 CFR Sections 160.103, 164.304, and 164.501.

A. HIPAA Regulations. "HIPAA Regulations" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules as set forth at 45 CFR Part 160 and Part 164.

B. Breach. "Breach" shall mean the acquisition, access, use, or disclosure of PHI in a manner not permitted under 45 CFR Part 164 Subpart E and that compromises the security or privacy of PHI as defined at 45 CFR Section 164.402.

C. Business Associate. "Business Associate" shall have the same meaning as the term "Business Associate" as set forth at 45 CFR Section 160.103.

D. Covered Entity. "Covered Entity" shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 CFR Section 160.103. For purposes of this Addendum, this term is intended to mean the County of Sonoma.

E. Data Aggregation. “Data Aggregation” shall have the same meaning as the term “Data aggregation” as set forth at 45 CFR Section 164.501.

F. Designated Record Set. “Designated Record Set” shall have the same meaning as the term “designated record set” as set forth at 45 CFR Section 164.501.

G. Disclosure. “Disclosure” shall mean the release of, transfer of, provision of access to, or divulging in any manner information outside the entity holding the information in accordance with 45 CFR Section 160.103.

H. Health Care Operations. “Health Care Operations” shall have the same meaning as “Health care operations” as set forth at 45 CFR Section 164.501.

I. Individual. “Individual” shall have the same meaning as the term "Individual" as set forth at 45 CFR Section 164.501, except that the term “Individual” as used in this Addendum shall also include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g).

J. Minimum Necessary. “Minimum Necessary” shall mean the minimum amount of PHI necessary for the intended purpose, as set forth at 45 CFR Sections 164.502(b) and 164.514(d): Standard: Minimum Necessary.

K. Privacy Rule. “Privacy Rule” shall mean the HIPAA Standards for Privacy of Individually Identifiable Health Information as set forth at 45 CFR Part 160 and 45 CFR Part 164 Subparts A and E.

L. PHI. “PHI” shall have the same meaning as the term “protected health information” as set forth at 45 CFR Section 160.103, except limited to the information received from Covered Entity or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

M. Required by Law. “Required by law” shall have the same meaning as the term “required by law” as set forth at 45 CFR Section 164.103.

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

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

P. Security Rule. “Security Rule” shall mean the HIPAA Security Standards for the Protection of ePHI as set forth at 45 CFR Part 160 and 45 CFR Part 164 Subparts A and E.

Q. Subcontractor. “Subcontractor” shall mean a subcontractor of Business Associate that creates, receives, maintains, or transmits PHI on behalf of Business Associate.

R. Unsecured PHI. "Unsecured PHI" shall have the same meaning as the term "unsecured protected health information" as set forth at 45 CFR Section 164.402, except limited to the information received from Covered Entity or created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity.

S. Use. "Use" shall mean, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information in accordance with 45 CFR Section 160.103.

2. Obligations of Business Associate

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

3. Use or Disclosure of Protected Health Information

Except as otherwise provided in Addendum, Business Associate shall use and/or disclose PHI only as necessary to perform functions, activities, or services documented in the Scope of Work ("Exhibit A") section of this Agreement for or on behalf of County, provided that such use and/or disclosure does not violate the HIPAA Regulations. . Business Associate agrees not to further use or disclose PHI other than as permitted or required by Addendum or as required by law. . Business Associate must make reasonable efforts to limit PHI to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request. The uses of PHI may not exceed the limitations applicable to County under the HIPAA Regulations.

4. Designation of a Privacy Officer and a Security Officer

A. Contractor shall designate a qualified and trained Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of the HIPAA Security Rule (45 CFR Part 164 Subpart C)

B. Contractor shall designate a qualified and trained Privacy Officer to oversee its information privacy program who shall be responsible for carrying out the requirements of the HIPAA Privacy Rule (45 CFR Part 164 et. seq.)

5. Safeguarding Protected Health Information

Business Associate shall use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by Addendum. Business Associate shall implement administrative, physical, and technical safeguards and shall comply with 45 CFR Part 164 Subpart C with respect to ePHI that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI created, received, maintained, or transmitted on behalf of County and prevent the use or disclosure of PHI other than as provided for by Agreement.

A. Encryption Requirements for Transmission and Storage of Electronic Data. All ePHI transmitted to Business Associate by County, and/or for or on behalf of County by Business Associate, and/or to County by Business Associate shall be provided or transmitted using encryption methods which renders such ePHI unusable, unreadable, or

indecipherable by unauthorized persons. All ePHI stored by Business Associate on electronic media shall be protected using encryption methods which render such ePHI unusable, unreadable, or indecipherable by unauthorized persons. Encryption of ePHI in transit or at rest shall use a technology or methodology set forth by the Secretary in the guidance issued under Section 13402(h)(2) of Public Law 111-5, and in accordance with the National Institute of Standards Technology (NIST) and Standards and Federal Information Processing Standards (FIPS), as applicable.

B. Destruction of PHI on paper, film, or other hard copy media must involve either shredding or otherwise destroying the PHI so that it cannot be read or reconstructed.

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

6. Notification of Breach, Unauthorized Use or Improper Disclosure

Business Associate must notify County in writing of any access, use, or disclosure of PHI not permitted or provided for by Addendum and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations of which Business Associate becomes aware. A breach or unauthorized access, use, or disclosure shall be treated as discovered by Business Associate the first day on which such unauthorized access, use, or disclosure is known, or should reasonably have been known, to Business Associate or to any person, other than the individual committing the unauthorized disclosure, that is an employee, officer, subcontractor, agent, or other representative of Business Associate.

A. Notification must be made as soon as practicable, but not later than 24 hours after discovery, by telephone call to 707-565-5703 plus e-mail to:

   DHS-Privacy&Security@sonoma-county.org, and will include:

   1) The identification of each Individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed; and

   2) A description of any remedial action taken or proposed to be taken by Business Associate.

B. Business Associate must provide a complete report of the investigation to the County Privacy and Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the County requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the County with such information.

C. Business Associate must mitigate any harm that results or may result from the breach, security incident, or unauthorized access, use, or disclosure of unsecured PHI by

Business Associate or its employees, officers, subcontractors, agents, or other representatives.

D. Following a breach or unauthorized access, use, or disclosure of unsecured PHI, Business Associate agrees to take any and all corrective action necessary to prevent recurrence, to document any such corrective action, and to make this documentation available to County.

7. Agents and Subcontractors of Business Associate

In accordance with 45 CFR Sections 164.502(e)(1)(ii) and 164.308(b)(2), and to the extent that Business Associate uses any agent, including a subcontractor, to which Business Associate provides PHI received from, created by, maintained by, or received by Business Associate on behalf of County, Business Associate shall execute an agreement with such agent or contractor containing a requirement to ensure compliance with the same restrictions and conditions that apply through Addendum to Business Associate with respect to PHI.

8. Access to Protected Health Information

At the request of County, and in the time and manner designated by County, Business Associate shall provide access to PHI in Designated Record Set to an Individual or County to meet the requirements of 45 CFR Section 164.524, and Ca. Health & Safety Code 123100 et. seq.

9. Amendments to Designated Record Set

Business Associate shall make any amendment(s) to PHI in Designated Record Set as directed or agreed to by County, or to take other measures necessary to satisfy County's obligations under 45 CFR Section 164.526.

10. Accounting of Disclosures

Business Associate shall document and make available such disclosures of PHI and information related to such disclosures as would be required for County to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528.

11. Records Available to County, State, and Secretary

Business Associate shall make available internal practices, books, and records related to the use, disclosure, and privacy protection of PHI received from County, or created, maintained, or received by Business Associate on behalf of County, to County, State, or the Secretary for the purposes of investigating or auditing Business Associate's compliance with the HIPAA Regulations in the time and manner designated by County, State, or Secretary.

12. Return or Destruction of Protected Health Information

A. Upon termination of Addendum for any reason, Business Associate shall:

1) Return all PHI received from County; return all PHI created, maintained or received by Business Associate on behalf of County; and return all PHI required to be retained by the HIPAA Regulations; OR:

2) at the discretion of County, destroy all PHI received from County, or created, maintained, or received by Business Associate on behalf of County. Destruction of PHI on paper, film, or other hard copy media must involve shredding or otherwise destroying the PHI in a manner which will render the PHI unreadable,

undecipherable, or unable to be reconstructed. Business Associate shall certify in writing that such PHI has been destroyed.

B. In the event Business Associate determines that returning or destroying PHI is not feasible, Business Associate shall provide County notification of the conditions that make return or destruction not feasible. Business Associate shall extend the protections of this Addendum to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

13. Data Aggregation

Business Associate may provide data aggregation services related to the health care operations of County as permitted by 45 CFR Section 164.504(e)(2)(i)(B).

14. Other Applicable Laws

Business Associate shall comply with all other applicable laws to the extent that such state confidentiality laws are not preempted by HIPAA.

15. Penalties/Fines for Failure to Comply with HIPAA

Business Associate shall pay any penalty or fine assessed against Covered Entity arising from Business Associate's failure to comply with the obligations imposed by HIPAA.

16. Training of Employees and Enforcement of Requirements

Business Associate shall train and use reasonable measures to ensure compliance with the requirements of this Business Associate Agreement by employees who assist in the performance of functions or activities on behalf of County under this Contract and use or disclose protected information; and discipline employees who intentionally violate any provisions.

17. Amendments to Addendum

No amendment of Addendum shall be effective unless and until such amendment is evidenced by a writing signed by the parties. County and Business Associate agree to take such action as is necessary to amend Addendum as required for County to comply with the requirements of the HIPAA Regulations. However, any provision required by HIPAA Regulations to be in Addendum shall bind the parties whether or not provided for in Addendum.

18. Termination of Addendum

If Business Associate should fail to perform any of its obligations hereunder, or materially breach any of the terms of Addendum, County may terminate Addendum immediately upon provision of notice stating the reason for such termination to Business Associate. County, within its sole discretion, may elect to give Business Associate an opportunity to cure such breach.

19. Material Breach

A breach by Business Associate or any of its agents or subcontractors of any provision of Addendum, as determined by County, shall constitute a material breach of Addendum and shall provide grounds for immediate termination of Addendum.

20. Indemnification

Business Associate agrees to accept all responsibility for loss or damage to any person or entity, including County, and to indemnify, hold harmless, and release County, its officers, agents, and employees from and against any actions, claims, damages, liabilities, disabilities, or expenses that may be asserted by any person or entity, including Business Associate, that arise out of, pertain to, or relate to Business Associate's or its agents', employees', contractors', subcontractors', or invitees' performance or obligations under Agreement. Business Associate agrees to provide a complete defense for any claim or action brought against County based upon a claim relating to such Business Associates' or its agents', employees', contractors', subcontractors', or invitees' performance or obligations under Agreement. Business Associates' obligations under Article 5 (Indemnification) apply whether or not there is concurrent negligence on County's part, but to the extent required by law, excluding liability due to County's conduct. County shall have the right to select its legal counsel at Business Associate's expense, subject to Business Associate's approval, which shall not be unreasonably withheld. This indemnification obligation is not limited in any way by any limitation on the amount or type of damages or compensation payable to or for Business Associate or its agents under workers' compensation acts, disability benefits acts, or other employee benefit acts.

Part II: Privacy and Security of Personal Information and Personally Identifiable Information Not Subject to HIPAA: (Applies to all contractors)

1. Recitals

A. In addition to the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the County is subject to various other legal and contractual requirements with respect to the personal information (PI) and personally identifiable information (PII) it maintains. These include:

   1) The California Information Practices Act of 1977 (California Civil Code §§ 1798 et seq.).

   2) The Agreement between the Social Security Administration (SSA) and the County, known as the Information Exchange Agreement (IEA), which incorporates the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency. The IEA, including the CMPPA, is attached to this Exhibit as Attachment B and is hereby incorporated in this Agreement.

B. The purpose of this Exhibit, Part II is to set forth Contractor’s privacy and security obligations with respect to PI and PII that Contractor may create, receive, maintain, use, or disclose for or on behalf of County pursuant to this Agreement. Specifically, this Exhibit applies to PI and PII which is not Protected Health Information (PHI) as defined by HIPAA and therefore is not addressed in this Exhibit, Part I of this Agreement, the HIPAA Business Associate Addendum.

C. The IEA Agreement referenced in A.2) above requires the County to extend its substantive privacy and security terms to subcontractors who receive data provided to DHCS by the Social Security Administration. If Contractor receives data from County that includes data provided to DHCS by the Social Security Administration, Contractor must comply with the following specific sections of the IEA Agreement: E. Security

Procedures, F. Contractor/Agent Responsibilities, and G. Safeguarding and Reporting Responsibilities for Personally Identifiable Information ("PII"), and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the Social Security Administration. Contractor must also ensure that any agents, including a subcontractor, to whom it provides County data that includes data provided by the Social Security Administration, agree to the same requirements for privacy and security safeguards for such confidential data that apply to Contractor with respect to such information.

D. The terms used in this Exhibit, Part II, but not otherwise defined, shall have the same meanings as those terms have in the above referenced statute and Agreement. Any reference to statutory, regulatory, or contractual language shall be to such language as in effect or as amended.

2. Definitions

A. "Breach" shall have the meaning given to such term under the IEA and CMPPA. It shall include a "PII loss" as that term is defined in the CMPPA.

B. "Breach of the security of the system" shall have the meaning given to such term under the California Information Practices Act, Civil Code § 1798.29(d).

C. Confidential Information shall mean information that is exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws

D. "CMPPA Agreement" means the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (CHHS).
https://www.ssa.gov/dataexchange/documents/CMPPA%20State%20Model.pdf

E. "County PI" shall mean Personal Information, as defined below, accessed in a database maintained by the County, received by Contractor from the County or acquired or created by Contractor in connection with performing the functions, activities and services specified in this Agreement on behalf of the County.

F. "IEA" shall mean the Information Exchange Agreement currently in effect between the Social Security Administration (SSA) and the California Department of Health Care Services (DHCS).
https://www.ssa.gov/dataexchange/documents/IEA(F)%20State%20Level.pdf

G. "Notice-triggering Personal Information" shall mean the personal information identified in Civil Code section 1798.29(e) whose unauthorized access may trigger notification requirements under Civil Code § 1709.29. For purposes of this provision, identity shall include, but not be limited to, name, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, a photograph or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper or any other medium.

H. "Personally Identifiable Information" (PII) shall have the meaning given to such term in the IEA and CMPPA.

I. "Personal Information" (PI) shall have the meaning given to such term in California Civil Code § 1798.3(a).

J. "Required by law" means a mandate contained in law that compels an entity to make a use or disclosure of PI or PII that is enforceable in a court of law. This 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, and a civil or an authorized investigative demand. It also includes 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 public benefits.

K. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PI, or confidential data utilized in complying with this Agreement; or interference with system operations in an information system that processes, maintains or stores PI.

L. Sensitive Information shall mean information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive Information may be either Public Information or Confidential Information. It is information that requires a higher than normal assurance of accuracy and completeness. Thus, the key factor for Sensitive Information is that of integrity. Typically, Sensitive Information includes records of agency financial transactions and regulatory actions.

3. Terms of Agreement

A. Permitted Uses and Disclosures of County PI and PII by Contractor

Except as otherwise indicated in this Exhibit, Part II, Contractor may use or disclose County PI only to perform functions, activities or services for or on behalf of the County pursuant to the terms of this Agreement provided that such use or disclosure would not violate the California Information Practices Act (CIPA) if done by the County.

B. Responsibilities of Contractor

Contractor agrees:

1) Nondisclosure. Not to use or disclose County PI or PII other than as permitted or required by this Agreement or as required by applicable state and federal law.

- The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure any Personal Information, Sensitive Information, or Confidential Information (hereinafter identified as PSCI).
- The Contractor and its employees, agents, or subcontractors shall not use any PSCI for any purpose other than carrying out the Contractor's obligations under this Agreement.
- The Contractor and its employees, agents, or subcontractors shall promptly transmit to the County Program Contract Manager all requests for disclosure of any PSCI not emanating from the person who is the subject of PSCI.

- The Contractor shall not disclose, except as otherwise specifically permitted by this Agreement or authorized by the person who is the subject of PSCI, any PSCI to anyone other than County without prior written authorization from the County Program Contract Manager, except if disclosure is required by State or Federal law.

2) Safeguards. To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of County PI and PII, to protect against anticipated threats or hazards to the security or integrity of County PI and PII, and to prevent use or disclosure of County PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which incorporate the requirements of Section 3, Security, below. Contractor will provide County with its current policies upon request.

3) Security. Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

   a) Complying with all of the data system security precautions listed in Part IV of this Special Terms and Conditions Document, Contractor Data Security Requirements; and

   b) Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

   c) If the data obtained by User(s) from County includes PII, User(s) shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement (IEA), which are attached as Attachment B and are incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. The User(s) also agree to ensure that any agents, including a subcontractor, to whom they provide County PII agree to the same requirements for privacy and security safeguards for confidential data that apply to the User(s) with respect to such information. The User(s) also agree to ensure that any agents, including a subcontractor, to whom they provide County PII agree to the same requirements for privacy and security safeguards for confidential data that apply to the User(s) with respect to such information.

4) Mitigation of Harmful Effects. To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of County PI or PII by Contractor or its subcontractors in violation of this Exhibit, Part II.

5) Contractor's Agents and Subcontractors. To impose the same restrictions and conditions set forth in this Exhibit, Part II on any subcontractors or other agents with whom Contractor subcontracts any activities under this Agreement that involve the disclosure of County PI or PII to the subcontractor.

6) Availability of Information to County. To make PI and PII available to the County for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of County PI and PII. If Contractor receives County PII, upon request by County, Contractor shall provide County with a list of all employees, contractors and agents who have access to County PII, including employees, contractors and agents of its subcontractors and agents.

7) Cooperation with County. With respect to County PI, to cooperate with and assist the County to the extent necessary to ensure the County's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of County PI, correction of errors in County PI, production of County PI, disclosure of a security breach involving County PI and notice of such breach to the affected individual(s).

8) Breaches and Security Incidents. During the term of this Agreement, Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

   a) Initial Notice to the County. (1) To notify the County immediately by telephone call plus email or fax upon the discovery of a breach of unsecured County PI or PII in electronic media or in any other media if the PI or PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon discovery of a suspected security incident involving County PII. (2) To notify the County within 24 hours (1 hour if SSA data) by email or fax of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of County PI or PII in violation of this Agreement or this Exhibit, Part I, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Contractor.

   b) Notice shall be provided to the County Privacy and Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic County PI or PII, notice shall be provided by calling the County Privacy and Security Officer. Notice shall be made using the County "Privacy Incident Report" form.

   c) Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of County PHI, Contractor shall take:

      i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

d) Investigation and Investigation Report. To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI within 72 hours of the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at the time, to the County Privacy and Security Officer.

e) Complete Report. To provide a complete report of the investigation to the County Privacy and Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the County requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the County with such information. If, because of the circumstances of the incident, Contractor needs more than ten (10) working days from the discovery to submit a complete report, the County may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The County will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.

f) Responsibility for Reporting of Breaches. If the cause of a breach of County PI or PII is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in CIPA, § 1798.29(a) – (d) and as may be required under the IEA. Contractor shall bear all costs of required notifications to individuals as well as any costs associated with the breach. The County Privacy and Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. The County will provide its review and approval expeditiously and without unreasonable delay. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the County in addition to Contractor, Contractor shall notify the County, and the County and Contractor may take appropriate action to prevent duplicate reporting.

g) County Contact Information. To direct communications to the above referenced County staff, the Contractor shall initiate contact as indicated herein. The County reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

Sonoma Co. Privacy Officer: 1450 Neotomas Ave. Suite 200, Santa Rosa, CA 95405; 707-565-5703; DHS-Privacy&Security@Sonoma-County.org

Part III: Miscellaneous Terms and Conditions including Access to 42 CFR Part 2 information. (Applies to all Contractors)

1. Confidentiality of Alcohol and Drug Abuse Patient Records

If Contractor is in possession or has access to information regulated by Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2, (42 CFR Part 2), Contractor shall comply with all related regulations. Contractor is aware that criminal penalties may be imposed for a violation of these confidentiality requirements.

2. Disclaimer

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

3. Amendment

A. The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Exhibit may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations. Upon either party's request, the other party agrees to promptly enter into negotiations concerning an amendment to this Exhibit embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations. The County may terminate this Agreement upon thirty (30) days written notice in the event:

    1) Contractor does not promptly enter into negotiations to amend this Exhibit when requested by the County pursuant to this section; or

    2) Contractor does not enter into an amendment providing assurances regarding the safeguarding of County PHI that the County deems necessary to satisfy the standards and requirements of HIPAA and the HIPAA regulations.

4. Judicial or Administrative Proceedings

Contractor will notify the County if it is named as a defendant in a criminal proceeding for a violation of HIPAA or other security or privacy law. The County may terminate this Agreement if Contractor is found guilty of a criminal violation of HIPAA. The County may terminate this Agreement if a finding or stipulation that the Contractor has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Contractor is a party or has been joined. County will consider the nature and seriousness of the violation in deciding whether or not to terminate the Agreement.

5. Assistance in Litigation or Administrative Proceedings

Contractor shall make itself and any subcontractors, employees or agents assisting Contractor in the performance of its obligations under this Agreement, available to the County at no cost to the

County to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the County, its directors, officers or employees based upon claimed violation of HIPAA, or the HIPAA regulations, which involves inactions or actions by the Contractor, except where Contractor or its subcontractor, employee or agent is a named adverse party.

6. No Third-Party Beneficiaries

Nothing express or implied in the terms and conditions of this Exhibit is intended to confer, nor shall anything herein confer, upon any person other than the County or Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

7. Interpretation

The terms and conditions in this Exhibit shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, and the HIPAA regulations. The parties agree that any ambiguity in the terms and conditions of this Exhibit shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations.

8. Conflict

In case of a conflict between any applicable privacy or security rules, laws, regulations or standards the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Contractor must comply within a reasonable period of time with changes to these standards that occur after the effective date of this Agreement.

9. Regulatory References

A reference in the terms and conditions of this Exhibit to a section in the HIPAA regulations means the section as in effect or as amended.

10. Survival

The respective rights and obligations of Contractor under Section 3, Item D of Exhibit, Part I, Responsibilities of Contractor, shall survive the termination or expiration of this Agreement.

11. No Waiver of Obligations

No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

12. Audits, Inspection and Enforcement

From time to time, and subject to all applicable federal and state privacy and security laws and regulations, the County may conduct a reasonable inspection of the facilities, systems, books and records of Contractor to monitor compliance with this Exhibit. Contractor shall promptly remedy any violation of any provision of this Exhibit. The fact that the County inspects, or fails to inspect, or has the right to inspect, Contractor’s facilities, systems and procedures does not relieve Contractor of its responsibility to comply with this Exhibit. The County's failure to detect a non-compliant practice, or a failure to report a detected non-compliant practice to Contractor does not constitute acceptance of such practice or a waiver of the County's enforcement rights under this Agreement, including this Exhibit.

13. Due Diligence

Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Exhibit.

14. Term

The Term of this Exhibit shall extend beyond the termination of the Agreement and shall terminate when all County PHI is destroyed or returned to the County, in accordance with 45 C.F.R. § 164.504(e)(2)(ii)(I), and when all County PI and PII is destroyed in accordance with Attachment A.

15. Effect of Termination

Upon termination or expiration of this Agreement for any reason, Contractor shall return or destroy all County PHI, PI and PII that Contractor still maintains in any form, and shall retain no copies of such PHI, PI or PII. If return or destruction is not feasible, Contractor shall notify the County of the conditions that make the return or destruction infeasible, and the County and Contractor shall determine the terms and conditions under which Contractor may retain the PHI, PI or PII. Contractor shall continue to extend the protections of this Exhibit to such County PHI, PI and PII, and shall limit further use of such data to those purposes that make the return or destruction of such data infeasible. This provision shall apply to County PHI, PI and PII that is in the possession of subcontractors or agents of Contractor.

Part IV: Contractor Data Security Requirements

1. General Controls

Contractor shall preserve and shall ensure that its sub-consultants or vendors preserve, the confidentiality, integrity, and availability of County data with administrative, technical and physical measures that conform to generally recognized industry standards and best practices that the selected firm then applies to its own processing environment. Maintenance of a secure processing environment includes, but is not limited to, the timely application of patches, fixes and updates to operating systems and applications as provided by Contractor and/or its sub-consultants or vendors. Contractor agrees to, and shall ensure that its sub-consultants or venders, comply with County's current and future information security policies, standards, procedures, and guidelines.

2. Designation of Individual(s) Responsible for information Privacy and Security

A. Security Officer:

Contractor shall designate a qualified individual, (HIPAA Security Officer), to implement and oversee its data security program. The individual shall be responsible for, and knowledgeable about, carrying out the requirements of this Special Terms and Conditions Exhibit, ensuring Contractor compliance with all provisions of the HIPAA Security Rule (45 CFR 164.300 et. seq.), and for communicating about privacy and security matters with the County.

B. Privacy Officer:

Contractor shall designate a qualified individual, (HIPAA Privacy Officer), to implement and oversee its information privacy program. The individual shall be responsible for, knowledgeable about, and trained in, carrying out the requirements of this Special Terms and Conditions Exhibit, ensuring Contractor compliance with all applicable state and federal information privacy laws (including but not limited to HIPAA, WIC 5328, 42 CFR Part 2, California Medical Information Act, etc.), and for communicating about privacy and security matters with the County.

C. The individual designated to the above roles may be the same individual so long as they are qualified and able to effectively perform the duties of both designations.

D. Any individual(s) designated as the Privacy Officer and/or Security Officer, must attend a Basic Privacy Compliance Academy course offered by the Health Care Compliance Association (HCCA) and obtain, within six (6) months of appointment, a "Certified in Healthcare Privacy Compliance" certification from the Health Care Compliance Association. Certification must be maintained continuously while designated in the role. Alternate training and certification may be considered equivalent if approved at the sole discretion of the County Privacy & Security Officer.

3. Personnel Controls

A. Employee Training. All workforce members who assist in the performance of functions or activities on behalf of the County, or access or disclose County PHI or PI must complete information privacy and security training, at least annually, at Contractor's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following termination of this Agreement.

B. Employee Discipline. Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

C. Confidentiality Statement. All persons that will be working with County PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to County PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for County inspection for a period of six (6) years following termination of this Agreement.

D. Background Check. Before a member of the workforce may access County PHI or PI, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years.

4. Technical Security Controls

A. Workstation/Laptop encryption. All workstations and laptops that store County PHI or PI either directly or temporarily must be encrypted using a FIPS 140-2 certified algorithm

which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the County Privacy and Security Office.

B. Server Security. Servers containing unencrypted County PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

C. Minimum Necessary. Only the minimum necessary amount of County PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

D. Removable media devices. All electronic files that contain County PHI or PI data must be encrypted when stored on any removable media or portable device (i.e.: USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

E. Antivirus software. All workstations, laptops and other systems that process and/or store County PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

F. Patch Management. All workstations, laptops and other systems that process and/or store County PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release. Applications and systems that cannot be patched within this time frame due to significant operational reasons must have compensatory controls implemented to minimize risk until the patches can be installed. Applications and systems that cannot be patched must have compensatory controls implemented to minimize risk, where possible.

G. User IDs and Password Controls. All users must be issued a unique user name for accessing County PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed at least every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

    1) Upper case letters (A-Z)
    2) Lower case letters (a-z)
    3) Arabic numerals (0-9)
    4) Non-alphanumeric characters (punctuation symbols)

H. Data Destruction. When no longer needed, all County PHI or PI must be wiped using the Gutmann or US Department of Defense (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 the County Privacy and Security Office.

I. System Timeout. The system providing access to County PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

J. Warning Banners. All systems providing access to County PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

K. System Logging. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for County PHI or PI, or which alters County PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If County PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

L. Access Controls. The system providing access to County PHI or PI must use role-based access controls for all user authentications, enforcing the principle of least privilege.

M. Transmission encryption. All data transmissions of County PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing County PHI can be encrypted. This requirement pertains to any type of County PHI or PI in motion such as website access, file transfer, and E-Mail.

N. Intrusion Detection. All systems involved in accessing, holding, transporting, and protecting County PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

5. Audit Controls

A. System Security Review. Contractor must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing County PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

B. Log Reviews. All systems processing and/or storing County PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

C. Change Control. All systems processing and/or storing County PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

D. Random Audits. Contractor will accommodate and upon reasonable notice by Sonoma County, work with Sonoma County and/or its subcontractors to submit to a random information security audit. This is to ensure that Contractor's and/or vendor's information security practices or standards comply with Sonoma County's information security policies, standards, procedures and guidelines. Contractor shall ensure that its sub-consultants or vendors comply with this requirement.

6. Business Continuity/Disaster Recovery Controls

A. Emergency Mode Operation Plan. Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of County PHI or PI held in an electronic format in the event of an emergency. Emergency means any

circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

B. Data Backup Plan. Contractor must have established documented procedures to backup County PHI to maintain retrievable exact copies of County PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore County PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of County data.

7. Paper Document Controls

A. Supervision of Data. County PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. County PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. Escorting Visitors. Visitors to areas where County PHI or PI is contained shall be escorted and County PHI or PI shall be kept out of sight while visitors are in the area.

C. Confidential Destruction. County PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

D. Removal of Data. Only the minimum necessary County PHI or PI may be removed from the premises of the Contractor except with express written permission of the County. County PHI or PI shall not be considered "removed from the premises" if it is only being transported from one of Contractor's locations to another of the same Contractor's locations.

E. Faxing. Faxes containing County PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

F. Mailing. Mailings containing County PHI or PI shall be sealed and secured from damage or inappropriate viewing of such PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of County PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of the County to use another method is obtained.

Part V: Provisions for Access to County Electronic Health Records System (Applies to contractors that have access to County E.H.R. system)

1. General Controls

AGREEMENTS AND CONDITIONS OF ACCESS AND USE In consideration for use of the Department of Health Services (DHS) Electronic Health Record system ("EHR"), User agrees to the following terms and conditions:

A. Contractor shall only use the EHR system to support clients served pursuant to a contract with the County.

B. Contractor and Contractor staff shall only access the EHR and Protected Health Information for the purpose of providing healthcare services.

C. Contractor shall ensure that staff will not use or disclose Protected Health Information other than as permitted or as required by law or this Agreement.

D. Contractor shall ensure that staff will not share or give authentication credentials, such as a USERID or password, to any other individual, or fail to take appropriate measures to safeguard their authentication credentials.

E. Contractor shall ensure that all staff with EHR access shall be trained on (i) the use of the EHR system; (ii) safeguards necessary to protect the EHR system, and (iii) the proper use/disclosure of information stored in the EHR system.

F. Contractor shall ensure that all staff with access to the EHR system sign a confidentiality agreement stating they will maintain confidentiality of protected information maintained in the EHR System. This agreement may be combined with other required confidentiality agreements.

G. Within 24 hours of discovery, Contractor shall report to DHS Privacy and Security Officer any use or disclosure of Protected Health Information which would violate State/federal regulations or the terms of this Agreement.

H. Contractor shall notify County of staff enrollment, staff changes job duties/credentialling, or staff separation from employment within 24 hours of the staff change using the form provided by the County.

I. County shall be responsible for enrollment of new staff into the EHR system, and adjustments to staff's level of access when staff changes job duties/credentialling or staff is separated from employment.

J. Contactor shall comply with all other information privacy and security provisions as articulated in this Agreement and exhibits.

K. If any use or disclosure of Protected Health Information by Contractor or Contractor's agents, staff, subcontractors, or invitees violates State/Federal regulations or the terms of this Agreement, Contractor agrees to accept all responsibility in accordance with Provision 19 (Indemnification) of the Business Associate Agreement.