MEMORANDUM OF UNDERSTANDING
BETWEEN
COMMUNITY ACTION PARTNERSHIP SOLANO, JOINT POWERS AUTHORITY,
PATHWAYS MISI
AND HMIS PARTNER AGENCIES

This Memorandum of Understanding (hereafter "MOU") is entered into as of _____, between the Community Action Partnership Solano Joint Powers Authority (hereafter "CAP Solano JPA"), on behalf of the Housing First Solano Continuum of Care, Pathways MISI, the Homeless Management Information System (HMIS) Administrator, and _____ (Partner Agency), referred to collectively as the Parties.

I. Background

Provisions in the U.S. Department of Housing and Urban Development's (HUD) Continuum of Care (CoC) Program and Emergency Solutions Grant (ESG) Program interim rules require that all CoCs establish and maintain a Homeless Management Information System (HMIS).

A HMIS is a client information system that maintains data for standardized assessments of consumer needs, individualized service plans, and use of housing and services. The HMIS database is intended as a shared database to enhance coordination and communication among Partner Agencies for the shared goal of increasing access to housing and services. The CAP Solano JPA and Housing First Solano Continuum of Care (HFS CoC) can also use this information to determine the utilization of services of participating agencies, identifying gaps in the local service continuum, develop outcome measurements, and to meet reporting requirements of the US Department of Housing and Urban Development (HUD).

The CAP Solano JPA is the HMIS Lead Agency for the HMIS system serving the HFS CoC. Pathways MISI is the HMIS Administrator selected by the CAP Solano JPA. Partner Agencies are Agencies which enter data into the HMIS.

II. Purpose

To ensure the consistent implementation of the HFS CoC HMIS policies and procedures, this MOU shall identify the obligations of the CAP Solano JPA, as the Collaborative Applicant for the HFS CoC, Pathways MISI, the HMIS Administrator, and Partner Agency that will enter data into HMIS.

III. Responsibilities of CAP Solano JPA:

CAP Solano JPA agrees to the following duties:

1. Designate and maintain a HMIS data system.
2. Designate and maintain a HMIS System Administrator, currently Pathways MISI.
3. Act as coordinating body for Partner Agencies and any other entity that participates in homeless services that may touch the HMIS System

4. Provide staff to the HMIS User Subcommittee.
5. Maintain HMIS policies and procedures.

IV. Responsibilities of Pathways MISI:

Pathways MISI, as the HMIS Administrator for the CAP Solano JPA on behalf of the HFS CoC, agrees to the following duties:

1. Provide technical assistance and support to Partner Agencies, Partner Agency Leads, and End Users.
2. Verify data produced by Partner Agency reporting is consistent with stipulations in relevant contracts with the CAP Solano JPA.
3. Create training materials that Partner Agencies can distribute to End Users.
4. Provide guidance and oversight to Partner Agencies surrounding required reporting, including Annual Performance Reports (APR) and Point-In-Time (PIT) Count process as it relates to HMIS.
5. Establish data quality standards in compliance with local and Federal Standards and support Partner Agencies in maintaining high quality data standards.
6. Ensure proper HMIS utilization and safe practices which may include audit of Partner Agency activities. If a Partner Agency fails to comply with this MOU or HMIS Policies and Procedures, Pathways MISI has the right to deny Partner Agency access to the HMIS until an appropriate resolution is enacted and agreed upon by all parties.

V. Responsibilities of Partner Agency:

Partner Agency, as a HMIS participating agency, agrees to the following duties:

1. Coordinate and support all users who will be entering data into HMIS (End Users) within the Partner Agency.
2. Ensure all End Users who are allowed access to the HMIS system are authorized by Partner Agency as necessary and appropriate to have access to client information and complete introductory and ongoing confidentiality and ethics training every 12 months provided by the HMIS Administrator, and have signed a Confidentiality and Security Agreement prior to receiving a User ID and Password.
3. Enter high quality, accurate data to the HMIS according to established timeframes.
4. Handle client data in accordance with privacy statutes and client requests, including:
    a. Uphold relevant federal, state and local confidentiality regulations and laws that protect client records.
    b. Meet or exceed organizational security standards contained in the HUD HMIS Data and Technical Standards, published in Federal Register volume 69 number 146 on July 30, 2004.
    a. Ensure the HMIS will not personally identify clients subject to the Violence Against Women Act (VAWA) including persons whose housing is impacted by the threat of domestic violence or are participating in programs that support victims of domestic violence.
    b. Execute a Business Associate Agreement (BAA) with the CAP Solano JPA (Exhibit A)
    c. Ensure confidential client information stored in the HMIS System is not shared without authorization.

d. Ensure that all clients whose information is stored in the HMIS have received a copy of the Notice of Privacy Practice (NPP), acknowledge the NPP and consent to their information being stored and accessed in HMIS. If consent is not provided, Partner Agency may still enter client information in HMIS, but must limit data sharing to Partner Agency only.
e. Maintain and post on its public website a Notice of Privacy Practice, and post a Privacy Statement at all service locations.

5. In the event of a breach of system security or client confidentiality, notify the HMIS Lead Agency and Pathways MISI within 24 hours of knowledge of such breach.
6. Identify a person to act as Partner Agency Lead. Duties of the Partner Agency Lead include:
    a. Liaise between the Partner Agencies, HMIS System administrator, and the CAP Solano JPA.
    b. Update System Administrator of all employee separations or role changes within 24 hours.
    c. Ensure new End Users are granted access to the HMIS by providing user access roles to HMIS System Administrator.
    d. Provide privacy, data sharing, and data quality oversight
    e. Ensure effective communication between End Users and HMIS System Administrator.
    f. Accept and process any HMIS related grievance procedures.
    g. Represent Partner Agency at HMIS User Subcommittee.
    h. Ensure the Partner Agency maintains compliance with this Participation Agreement and all other documents, agreements, and policies surrounding the administration of the HMIS.

VI. Cost

Partner Agency agrees to pay an annual fee to use the HMIS system and understands that the CAP Solano will establish a per user license cost based on systems costs and notify Partner Agencies of the cost at the time of request or renewal. Partner Agencies may request a subsidy for user fees by submitting a subsidy request form and will be approved at the sole discretion of the CAP Solano JPA.

VII. *Terms of Agreement*:

This MOU shall be in effect from the date marked herein until such a time as either party submits a notice of termination or signs an updated version of this agreement. Written notices of termination submitted by either party will take effect 90 days following receipt.

Modification. This MOU can be expanded, modified, or amended, as needed, at any time by the written consent of all parties. This MOU shall be reviewed and revised as needed for further implementation of any strategic and long-term goals of the project.

Liability. The CAP Solano JPA and the participating agency each agree to defend, indemnify, and hold each other harmless from any claims or liability arising from the acts or omissions of the other, including any third-party claims arising from the acts or omissions of any officers, employees, agents, representatives, licensees, or clients of the other. The CAP Solano JPA shall not be liable for any injuries or other claims that arise

from events that occur at the designated entry points.

Severability. The invalidity or unenforceability of any particular provision of this MOU shall not affect the remaining provisions hereof, and the MOU shall be construed in all respects as if such invalid or enforceable provision were omitted.

IN WITNESS, WHEREOF the Parties entered into this Agreement as of the Effective Date.

Partner Agency

Agency: _____

Address: _____

Name: _____

Title: _____

Signature: _____

Date: _____

CAP Solano JPA

Name: _____

Title: _____

Signature: _____

Date: _____

Pathways MISI

Name: _____

Title: _____

Signature: _____

Date: _____

HMIS Partner Agency MOU Exhibit A
Business Associate Agreement

This Exhibit shall constitute the Business Associate Agreement (the "Agreement") between the Community Action Partnership Joint Powers Authority (CAP Solano JPA) and the Partner Agency and applies to the data Partner Agency will supply in the Homeless Management Information System (HMIS).

A. The CAP Solano JPA and Partner Agency wish to disclose certain information to pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI") (defined below).

B. The CAP Solano JPA and Partner Agency acknowledge that Partner Agency is subject to the Privacy and Security Rules (45 CFR parts 160 and 164) promulgated by the United States Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 as amended by the Health Information Technology for Economic and Clinical Health Act as set forth in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 ("HITECH Act), in certain aspects of its operations performed on behalf of the CAP Solano JPA.

C. As part of the HIPAA Regulations, the Privacy Rule and the Security Rule (defined below) require the CAP Solano JPA to enter into an Agreement containing specific requirements with Partner Agency prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, sections 164.314(a), 164.502(e) and 164.504(e) of the Code of Federal Regulations ("C.F.R.") and contained in this Agreement.

1. DEFINITIONS

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 CFR parts 160 and 164.

1. Breach means the same as defined under the HITECH Act [42 U.S.C. section 17921].

2. Contractor means the same as defined under the Privacy Rule, the Security rule, and the HITECH Act, including, but not limited to, 42 U.S.C. section 17938 and 45 C.F.R. § 160.103.

3. Breach of the Security of the Information System means the unauthorized acquisition, including, but not limited to, access to, use, disclosure, modification or destruction, of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by or on behalf of the CAP Solano JPA. Good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system; provided, that the personal information is not used or subject to further unauthorized disclosure.

4. Commercial Use means obtaining protected health information with the intent to sell, transfer or use it for commercial, or personal gain, or malicious harm; sale to third party for consumption, resale, or processing for resale; application or conversion of data to make a profit or obtain a benefit contrary to the intent of this Agreement.

5. Covered Entity means the same as defined under the Privacy Rule and the Security rule, including, but not limited to, 45 C.F.R. § 160.103.

6. Designated Record Set means the same as defined in 45 C.F.R. § 164.501.

7. Electronic Protected Health Information (ePHI) means the same as defined in 45 C.F.R. § 160.103.

8. Electronic Health Record means the same as defined shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. § 17921.

9. Encryption means the process using publicly known algorithms to convert plain text and other data into a form intended to protect the data from being able to be converted back to the original plain text by known technological means.

10. Health Care Operations means the same as defined in 45 C.F.R. § 164.501.

11. Individual means the same as defined in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

12. Marketing means the same as defined under 45 CFR § 164.501 and the act or process of promoting, selling, leasing or licensing any patient information or data for profit without the express written permission of the CAP Solano JPA.

13. Privacy Officer means the same as defined in 45 C.F.R. § 164.530(a)(1). The Privacy Officer is the official designated to be responsible for compliance with HIPAA/HITECH regulations.

14. Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR parts 160 and t 164, subparts A and E.

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

16. Required By Law means the same as defined in 45 CFR § 164.103.

17. Security Rule means the HIPAA Regulation that is codified at 45 C.F.R. parts 160 and 164, subparts A and C.

18. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

19. Security Event means an immediately reportable subset of security incidents which incident would include:

    a. a suspected penetration of Partner Agency's information system of which the Partner Agency becomes aware of but for which it is not able to verify immediately upon becoming aware of the suspected incident that PHI was not accessed, stolen, used, disclosed, modified, or destroyed;

    b. any indication, evidence, or other security documentation that the Partner Agency's network resources, including, but not limited to, software, network routers, firewalls, database and application servers, intrusion detection systems or other security appliances, may have been damaged, modified, taken over by proxy, or otherwise compromised, for which Partner Agency cannot refute the indication of the time the Partner Agency became aware of such indication;

    c. a breach of the security of the Partner Agency's information system(s) by unauthorized acquisition, including, but not limited to, access to or use, disclosure, modification or destruction, of unencrypted computerized data and which incident materially compromises the security, confidentiality, or integrity of the PHI; and or,

    d. the unauthorized acquisition, including but not limited to access to or use, disclosure, modification or destruction, of unencrypted PHI or other confidential information of the HMIS by an employee or authorized user of Partner Agency's system(s) which materially compromises the security, confidentiality, or integrity of PHI or other confidential information of the CAP Solano JPA.

If data acquired (including but not limited to access to or use, disclosure, modification or destruction of such data) is in encrypted format but the decryption key which would allow the decoding of the data is also taken, the parties shall treat the acquisition as a breach for purposes of determining appropriate response.

20. Security Rule means the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR parts 160 and 164, subparts A and C.

21. Unsecured PHI means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary. Unsecured PHI shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. section 17932(h).

2. OBLIGATIONS OF PARTNER AGENCY

1. Compliance with the Privacy Rule: Partner Agency agrees to fully comply with the requirements under the Privacy Rule applicable to "Business Associates" as defined in the Privacy Rule and not use or further disclose Protected Health Information other than as permitted or required by this agreement or as required by law.

2. Compliance with the Security Rule: Partner Agency agrees to fully comply with the requirements under the Security Rule applicable to "Business Associates" as defined in the Security Rule.

3. Compliance with the HITECH Act: Partner Agency hereby acknowledges and agrees it will comply with the HITECH provisions as proscribed in the HITECH Act.

III. USES AND DISCLOSURES

Partner Agency shall not use Protected Health Information except for the purpose of performing Partner Agency's obligations under the MOU and as permitted by the MOU and this Agreement. Further, Partner Agency shall not use Protected Health Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so used by the CAP Solano JPA.

1. Partner Agency may use Protected Health Information:

    a. For functions, activities, and services for or on the Covered Entities' behalf for purposes specified in the MOU and this Agreement.

    b. As authorized for Partner Agency's management, administrative or legal responsibilities as a Partner Agency of the CAP Solano JPA. The uses and disclosures of PHI may not exceed the limitations applicable to the CAP Solano JPA;

    c. As required by law.

    d. To provide Data Aggregation services to the CAP Solano JPA as permitted by 45 CFR § 164.504(e)(2)(i)(B).

    e. To report violations of law to appropriate Federal and State authorities, consistent with CFR § 164.502(j)(1).

2. Any use of Protected Health Information by Partner Agency, its agents, or subcontractors, other than those purposes of the Agreement, shall require the express written authorization by the CAP Solano JPA and a Business Associate Agreement or amendment as necessary.

3. Partner Agency shall not disclose Protect Health Information to a health plan for payment or health care operations if the patient has requested this restriction and has paid out of pocket in full for the health care item or service to which the

Protected Health information relates.

4. Partner Agency shall not directly or indirectly receive remuneration in exchange for Protected Health Information, except with the prior written consent of the CAP Solano JPA and as permitted by the HITECH Act, 42 U.S.C. section 17935(d)(2); however, this prohibition shall not affect payment by the CAP Solano JPA to Partner Agency for services provided pursuant to the Contract.

5. Partner Agency shall not use or disclose Protected Health Information for prohibited activities including, but not limited to, marketing or fundraising purposes.

6. Partner Agency agrees to adequately and properly maintain all Protected Health Information received from, or created, on behalf of the CAP Solano JPA.

7. If Partner Agency discloses Protected Health Information to a third party, Partner Agency must obtain, prior to making any such disclosure, i) reasonable written assurances from such third party that such Protected Health Information will be held confidential as provided pursuant to this Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify the Partner Agency of any breaches of confidentiality of the Protected Health Information, to the extent it has obtained knowledge of such breach [42 U.S.C. section 17932; 45 C.F.R. §§ 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)].

IV. MINIMUM NECESSARY

Partner Agency (and its agents or subcontractors) shall request, use and disclose only the minimum amount of Protected Health necessary to accomplish the purpose of the request, use or disclosure. [42 U.S.C. section 17935(b); 45 C.F.R. § 164.514(d)(3)]. Partner Agency understands and agrees that the definition of "minimum necessary" is in flux and shall keep itself informed of guidance issued by the Secretary with respect to what constitutes "minimum necessary."

V. APPROPRIATE SAFEGUARDS

1. Partner Agency shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Health Information otherwise than as permitted by this Agreement, including, but not limited to, administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Health Information in accordance with 45 C.F.R. §§ 164.308, 164.310, and 164.312. [45 C.F.R. § 164.504(e)(2)(ii)(B); 45 C.F.R. § 164.308(b)]. Partner Agency shall comply with the policies and procedures and documentation requirements of the HIPAA Security Rule, including, but not limited to, 45 C.F.R. § 164.316. [42 U.S.C. section 17931].

2. Partner Agency agrees to comply with Subpart 45 CFR part 164 with respect to Electronic Protected Health Information (ePHI). Partner Agency must secure all Electronic Protected Health Information by technological means that render such information unusable, unreadable, or indecipherable to unauthorized individuals

and in accordance with the National Institute of Standards Technology (NIST) Standards and Federal Information Processing Standards (FIPS) as applicable.

3. Partner Agency agrees that destruction of Protected Health Information on paper, film, or other hard copy media must involve either cross cut shredding or otherwise destroying the Protected Health Information so that it cannot be read or reconstructed.

4. Should any employee or subcontractor of Partner Agency have direct, authorized access to computer systems of the CAP Solano JPA that contain Protected Health Information, Partner Agency shall immediately notify the CAP Solano JPA 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 the CAP Solano JPA to disable previously authorized access.

VI. AGENT AND SUBCONTRACTOR'S OF PARTNER AGENCY

1. Partner Agency shall ensure that any agents and subcontractors to whom it provides Protected Health Information, agree in writing to the same restrictions and conditions that apply to Partner Agency with respect to such PHI and implement the safeguards required with respect to Electronic PHI [45 C.F.R. § 164.504(e)(2)(ii)(D) and 45 C.F.R. § 164.308(b)].

2. Partner Agency shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation (see 45 C.F.R. §§ 164.530(f) and 164.530(e)(I)).

VII. ACCESS TO PROTECTED HEALTH INFORMATION

1. If Partner Agency receives Protected Health Information from the CAP Solano JPA in a Designated Record Set, Partner Agency agrees to provide access to Protected Health Information in a Designated Record Set to the CAP Solano JPA in order to meet its requirements under 45 C.F.R. § 164.524.

2. Partner Agency shall make Protected Health Information maintained by Partner Agency or its agents or subcontractors in Designated Record Sets available to CAP Solano JPA for inspection and copying within five (5) days of a request by CAP Solano JPA to enable the CAP Solano JPA to fulfill its obligations under state law, [Health and Safety Code section 123110] the Privacy Rule, including, but not limited to, 45 C.F.R. § 164.524 [45 C.F.R. § 164.504(e)(2)(ii)(E)]. If Partner Agency maintains an Electronic Health Record, Partner Agency shall provide such information in electronic format to enable the CAP Solano JPA to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. section 17935(e).

3. If Partner Agency receives a request from an Individual for a copy of the individual's Protected Health Information, and the Protected Health Information is in the sole possession of the Partner Agency, Partner Agency will provide the requested copies to the individual in a timely manner. If Partner Agency receives a request for

Protected Health Information not in its possession and in the possession of the CAP Solano JPA, or receives a request to exercise other individual rights as set forth in the Privacy Rule, Partner Agency shall promptly forward the request to the CAP Solano JPA. Partner Agency shall then assist the CAP Solano JPA as necessary in responding to the request in a timely manner. If a Partner Agency provides copies of Protected Health Information to the individual, it may charge a reasonable fee for the copies as the regulations shall permit.

4. Partner Agency shall provide copies of HIPAA Privacy and Security Training records and HIPAA policies and procedures within five (5) calendar days upon request from the CAP Solano JPA.

VIII. AMENDMENT OF PROTECTED HEALTH INFORMATION

Upon receipt of notice from the CAP Solano JPA, promptly amend or permit the CAP Solano JPA access to amend any portion of Protected Health Information in the designated record set which Partner Agency created for or received from the CAP Solano JPA so that the CAP Solano JPA may meet its amendment obligations under 45 CFR § 164.526. If any individual requests an amendment of Protected Information directly from Partner Agency or its agents or subcontractors, Partner Agency must notify the CAP Solano JPA in writing within five (5) days of the request. Any approval or denial of amendment of Protected Information maintained by Partner Agency or its agents or subcontractors shall be the responsibility of the CAP Solano JPA [45 C.F.R. § 164.504(e)(2)(ii)(F)].

IX. ACCOUNTING OF DISCLOSURES

1. At the request of the CAP Solano JPA, and in the time and manner designed by the CAP Solano JPA, Partner Agency and its agents or subcontractors shall make available to the CAP Solano JPA, the information required to provide an accounting of disclosures to enable the CAP Solano JPA to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. § 164.528, and the HITECH Act, including but not limited to 42 U.S.C. § 17935. Partner Agency agrees to implement a process that allows for an accounting to be collected and maintained by the Partner Agency and its agents or subcontractors for at least six (6) years prior to the request. However, accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for only three (3) years prior to the request, and only to the extent that Partner Agency maintains an electronic health record and is subject to this requirement.

2. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Health Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure.

3. In the event that the request for an accounting is delivered directly to Partner

Agency or its agents or subcontractors, Partner Agency shall forward within five (5) calendar days a written copy of the request to the CAP Solano JPA. It shall be the CAP Solano JPA's responsibility to prepare and deliver any such accounting requested. Partner Agency shall not disclose any Protected Information except as set forth in this Agreement [45 C.F.R. §§ 164.504(e)(2)(ii)(G) and 165.528]. The provisions of this paragraph shall survive the termination of this Agreement.

X. GOVERNMENTAL ACCESS TO RECORDS

Partner Agency shall make its internal practices, books and records relating to its use and disclosure of the protected health information it creates for or receives from the CAP Solano JPA, available to the CAP Solano JPA and to the Secretary of the U.S. Department of Health and Human for purposes of determining Partner Agency's compliance with the Privacy rule [45 C.F.R. § 164.504(e)(2)(ii)(H)]. Partner Agency shall provide to the CAP Solano JPA a copy of any Protected Health Information that Partner Agency provides to the Secretary concurrently with providing such Protected Information to the Secretary.

XI. CERTIFICATION

To the extent that the CAP Solano JPA determines that such examination is necessary to comply with the Partner Agency's legal obligations pursuant to HIPAA relating to certification of its security practices, the CAP Solano JPA, or its authorized agents Contractor may, at the CAP Solano JPA's expense, examine Partner Agency's facilities, systems, procedures and records as may be necessary for such agents or Contractor to certify to the CAP Solano JPA the extent to which Partner Agency's security safeguards comply with HIPAA Regulations, the HITECH Act, or this Agreement.

XII. BREACH OF UNSECURED PROTECTED HEALTH INFORMATION

1. In the case of a breach of unsecured Protected Health Information, Partner Agency shall comply with the applicable provisions of 42 U.S.C. § 17932 and 45 C.F.R. part 164, subpart D, including but not limited to 45 C.F.R. § 164.410.

2. Partner Agency agrees to notify the CAP Solano JPA of any access, use or disclosure of Protected Health Information not permitted or provided for by this Agreement of which it becomes aware, including any breach as required in 45 45 C.F.R. § 164.410. or security incident immediately upon discovery and will include, to the extent possible, the identification of each Individual whose unsecured Protected Health Information has been, or is reasonably believed by the Partner Agency to have been accessed, acquired, used, or disclosed, a description of the Protected Health Information involved, the nature of the unauthorized access, use or disclosure, the date of the occurrence, and a description of any remedial action taken or proposed to be taken by Partner Agency. Partner Agency will also provide to the CAP Solano JPA any other available information that the Covered entity requests.

3. A breach or unauthorized access, use or disclosure shall be treated as discovered by the Partner Agency on the first day on which such unauthorized access, use, or disclosure is known, or should reasonably have been known, to the Partner Agency or to any person, other than the individual committing the unauthorized disclosure,

that is an employee, officer, subcontractor, agent or other representative of the Partner Agency.

4. Partner Agency shall mitigate, to the extent practicable, any harmful effect that results from a breach, security incident, or unauthorized access, use or disclosure of unsecured Protected Health Information by Partner Agency or its employees, officers, subcontractors, agents or representatives.

5. Following a breach, security incident, or any unauthorized access, use or disclosure of unsecured Protected Health Information, Partner Agency agrees to take any and all corrective action necessary to prevent recurrence, to document any such action, and to make all documentation available to the CAP Solano JPA.

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

7. Partner Agency acknowledges that it is required to comply with the referenced rules and regulations and that Partner Agency (including its subcontractors) may be held liable and subject to penalties for failure to comply.

8. In meeting its obligations under this Agreement, it is understood that Partner Agency is not acting as the CAP Solano JPA's agent. In performance of the work, duties, and obligations and in the exercise of the rights granted under this Agreement, it is understood and agreed that Partner Agency is at all times acting an independent Partner Agency in providing services pursuant to this Agreement and Exhibit A, Scope of Work.

XIII. TERMINATION OF AGREEMENT

1. Upon termination of this Agreement for any reason, Partner Agency shall return or destroy, at the CAP Solano JPA's sole discretion, all other Protected Health Information received from the CAP Solano JPA, or created or received by Partner Agency on behalf of the CAP Solano JPA.

2. Partner Agency will retain no copies of Protected Health Information in possession of subcontractors or agents of Partner Agency.

3. Partner Agency shall provide the CAP Solano JPA notification of the conditions that make return or destruction not feasible, in the event that Partner Agency determines that returning or destroying the PHI is not feasible. If the CAP Solano

JPA agrees that the return of the Protected Health Information is not feasible, Partner Agency shall extend the protections of this Agreement to such Protected Health Information and limit further use and disclosures of such Protected Health Information for so long as the Partner Agency or any of its agents or subcontractor maintains such information.

4. Partner Agency agrees to amend this Exhibit as necessary to comply with any newly enacted or issued state or federal law, rule, regulation or policy, or any judicial or administrative decision affecting the use or disclosure of Protected Health Information.

5. Partner Agency agrees to retain records, minus any Protected Health Information required to be returned by the above section, for a period of at least 7 years following termination of the Agreement. The determining date for retention of records shall be the last date of encounter, transaction, event, or creation of the record.

XIV. CERTIFICATION

I, the official named below, certify that I am duly authorized legally to bind the Partner Agency to the above described certification. I am fully aware that this certification is made under penalty of perjury under the laws of the State of California.

_____

Partner Agency Date

_____

Official's Name (type or print)

_____

Title Federal Tax ID Number