SONOMA COUNTY HOMELESS COALITION
HOMELESS MANAGEMENT INFORMATION SYSTEM

Participation Agreement

This Sonoma County Homeless Coalition Homeless Management Information System ("HMIS") Participation Agreement ("Agreement"), dated as of _____, _____, is by and between the County of Sonoma Department of Health Services ("Administrator" or "DHS"), with offices located at 1450 Neotomas Avenue, Suite 200, Santa Rosa, CA 95405, and <Agency Name>, a California non-profit corporation ("Participant"), with principal offices located at <Agency Address>.

RECITALS

WHEREAS, the parties have a mutual goal to enhance collaborative efforts to improve service delivery to homeless individuals and families; and

WHEREAS, the parties acknowledge that shared information is a key factor in achieving this goal; and

WHEREAS, Participants and DHS desire to improve services for the benefit of Sonoma County residents; and

WHEREAS, HMIS is designed to assist in achieving this goal; and

WHEREAS, the United States Congress has mandated that all recipients of McKinney-Vento Homelessness Assistance Funding implement an HMIS by October 2004; and

WHEREAS, Participants have requested that DHS function as lead agency for the Sonoma County HMIS and DHS has agreed to function as lead agency for the Sonoma County HMIS.

NOW, THEREFORE in consideration of the mutual provisions contained herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Administrator and Participant hereby agree as follows:

1. Definitions
   a. "Agency Administrator" means the single staff person in each Partner Agency designated by that agency to be the HMIS software administrator for that agency and who, as a result of that designation, has specialized training and a higher level of data access.
   b. "Blind Service Providers" means agencies serving specific protected client populations, which typically have one or more of the following issues: (1) domestic violence, (2) HIV/AIDS, (3) Alcohol and/or substance abuse, and/or (4) mental health.
   c. "Client" means a consumer of services from a Provider.
   d. "Client records" means Private Personal Information (PPI) about a client, which is collected and stored in a computer system.
   e. "Close to real-time data entry" means data entry within five (5) working days of serving a Client.
   f. "Partner Agencies" means agencies that work together and provide services to homeless and low-income individuals and families and that participate in the HMIS.

g. "HMIS Administrator" means the DHS employee assigned to manage the HMIS Collaborative Project.

h. "Non-partner agencies" means those agencies not participating in the HMIS.

2. 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. Privacy and Security of Personal and Personally Identifiable Information

3. Participation Fee. Each Participant shall be charged an annual participation fee to be involved in the HMIS. The annual fee shall be invoiced by and payable to DHS. The amount of the participation fee shall be determined by the Sonoma County Homeless Coalition Board after recommendation by the HMIS Data Committee, an advisory committee of the Homeless Coalition Board.

a. Participation Fees are outlined in the Homeless Coalition Governance Charter and can be located online by using the following link: https://sonomacounty.ca.gov/health-and-human-services/health-services/divisions/homelessness-services/sonoma-county-homeless-coalition/coc-governance-and-compliance.

4. Confidentiality. DHS and Participant agree that the data, information, client records, and related documentation, stored electronically in connection with the HMIS, is confidential and shall be handled as follows:

a. The Participant shall comply with all federal, state, and local laws and regulations pertaining to the confidentiality of information and records to ensure that client records are protected and not subject to disclosure except as permitted by such laws and regulations. The Participant shall release client records only to Non-partner agencies with written consent by the client, unless otherwise provided in the relevant laws and regulations.

b. The Participant shall comply with all federal, state, and local confidentiality laws and regulations pertaining to:

1) All medical conditions, including but not limited to, mental illness, alcohol and/or drug abuse, HIV/AIDS testing, diagnosis, treatment, and other such covered conditions; and

2) A person's status as a victim of domestic violence.

c. Federal, state, and local laws may protect the privacy of and the confidentiality of information and documents relating to persons with physical and/or mental illness, persons who have been treated for alcohol and/or substance abuse, persons who have been diagnosed with HIV/AIDS, and/or persons who have been a victim of domestic violence. The Participant agrees that it shall seek legal advice in the event that a Non-partner agency or other third party requests client records.

d. The Participant shall provide to each Client a verbal explanation of the HMIS database and the general terms of the consent sought from the Client in connection with the HMIS. The Participant shall arrange for a qualified interpreter or translator in the event that an individual is not fluent in English or has difficulty understanding the consent form.

e. The Participant agrees not to release any individual client information obtained from the HMIS to any organization or individual without prior written consent of the Client, unless otherwise required or permitted by applicable law or regulation. Such written Client consent shall specify exactly what information the Client allows to be released. Information that is not approved for disclosure in writing by the Client shall not be released. The Participant shall allow a Client to inspect and copy the Client's own protected information within thirty (30) days of the Client's written request to the Participant.

f. The Participant shall ensure that all staff, volunteers, and other persons who are issued a User ID and password for the HMIS receive confidentiality training regarding client information and records and have signed a Confidentiality and Security Agreement.

g. If Participant or DHS determines that any staff, volunteer, or other person who has been granted a User ID and password has willfully committed a breach of HMIS system security or client confidentiality, Participant or DHS shall immediately revoke their access to the HMIS database. DHS may review Participant's policies, procedures, and records to ensure that individuals found to have willfully committed a breach of HMIS system security or client confidentiality are prohibited from accessing the HMIS system.

h. In the event of a breach of HMIS system security or client confidentiality, the Participant shall notify the HMIS Administrator within 24 hours. If the HMIS Manager determines that a Participant employee or volunteer has breached the HMIS system security or client confidentiality, the Participant shall enter a period of probation. During the probationary period, the HMIS Administrator shall provide technical assistance to help the Participant prevent further breaches. Probation shall remain in effect until the HMIS Administrator Manager has evaluated the Participant's security and confidentiality measures and found them to be compliant with the policies stated in this Agreement and the Confidentiality and Security Agreement. Subsequent violations of system security or client confidentiality may result in Participant being suspended from the HMIS system. DHS reserves the right to conduct routine and random audits to monitor HMIS system security and client confidentiality.

i. The HMIS fileserver, which contains all HMIS-entered Client information, shall be located off-site in a physically secure and electronically monitored facility, and client information in the HMIS system shall be backed up and taken off-site daily. The Participant understands that the fileserver containing all HMIS-entered Client information is maintained by a vendor contracting with DHS to provide said services. The contractor vendor has access to client information, said access being necessary to provide technical services to DHS that are necessary to operate the HMIS. The contractor has agreed to keep all information confidential and maintained in accordance with HUD privacy standards.

j. The Participant may have access to all Client data entered by the Participant. The Participant shall diligently record in the HMIS all service delivery information pertaining to individual clients served by the Participant. The Participant shall not under any circumstances knowingly enter false, misleading, or biased data, including any data that would unfairly prejudice a Client's ability to obtain services.

k. If this Agreement is terminated, the remaining Partner Agencies shall maintain their right to the use of all Client data previously entered by the terminating Partner Participant, subject to the guidelines specified in this Agreement.

l. The Participant shall utilize the HMIS and Coordinated Entry System Consent for the Release of Confidential Information form for all Clients providing information to the HMIS. The HMIS and Coordinated Entry System Consent for the Release of Confidential Information form, once agreed to and signed by the Client, authorizes Client data to be shared with Partner Agencies for a period of three (3) years, subject to the restrictions defined by the form.

m. All Participants shall use the common consent form that is in compliance with HUD requirements.

n. The Participant shall keep original signed copies of the HMIS and Coordinated Entry System Consent for the Release of Confidential Information form for a period of no less than five (5) years.

o. The Participant shall not state or imply to the Client that HMIS requires a Client's participation in the HMIS database. The Participant shall provide services to a Client even if Client declines to participate in HMIS or execute the Client Consent form, provided the Client would otherwise be eligible for the services.

p. The Participant shall have access to identifying and statistical data on all Clients who consent to have their information entered in the HMIS database, except for data input into the database by Blind Service Providers.

q. A Participant that is a Blind Service Provider shall have access to identifying and statistical data that the Participant inputs into the HMIS database only for Clients served by that Participant.

r. A Participant that is a Blind Service Provider shall not have access to identifying and statistical data input into the HMIS database for clients served by other Blind Service Providers.

5. HMIS Use, Data Entry, and System Security. The Participant agrees to use the HMIS, enter data into the HMIS, and operate the HMIS so as to protect the integrity of the HMIS and the confidentiality of the data in the HMIS, and so as to comply with the following guidelines:

a. The Participant shall comply with and enforce all provisions contained in the Confidentiality and Security Agreement. Modifications to the Confidentiality and Security Agreement shall be established in consultation with Partner Agencies and may be modified as needed for the smooth and efficient operation of the HMIS or to accommodate changes in law or regulation.

b. The Participant shall enter only true and accurate data in the HMIS database relating to actual, existing Clients served by the Participant. The Participant shall not misrepresent its Client base in the HMIS database by knowingly entering inaccurate information. The Participant shall not use the HMIS database with the intent to defraud federal, state, or local governments, individuals or entities, or to conduct any illegal activity.

c. The Participant shall use Client information in the HMIS, as provided to the Participant or the Partner Agencies, solely to assist the Participant in providing

adequate and appropriate services to the Client and in meeting required reporting obligations.

d. The Participant shall promptly and consistently enter information into the HMIS database and shall strive for real-time data entry or close to real-time data entry.

e. When a Client revokes their consent to share information in the HMIS database, the User shall immediately notify the Agency Administrator of the revocation. When the Agency Administrator is notified of a client revocation, the Agency Administrator shall immediately remove access to all personally identifying information about that client.

f. The Participant shall not include profanity or offensive language in the HMIS database.

g. The Participant shall utilize the HMIS only for client services and mandated reporting purposes.

h. The HMIS Administrator shall provide or arrange for introductory training to Participant staff on the use of the HMIS software. The HMIS Administrator shall provide or arrange for supplemental training regularly to accommodate changes in Participant staff and address modifications to the software when needed.

i. The HMIS Administrator shall be available to provide or arrange for technical assistance to Participant staff.

j. The Participant shall ensure that all staff, volunteers, and other persons who are issued a User ID and password for HMIS receive client and system security training that covers established user policies, standards, responsibilities, and ethics.

k. The Participant shall take the following additional steps to ensure the security of the HMIS database system and the confidentiality of Client data:

    1) Escort all visitors and Clients to ensure that they do not access staff areas, record storage areas, or other areas potentially containing Client information. Persons not recognized as staff, visitors, and Clients shall be asked for identification.

    2) Store hard copies of Client records in locking filing cabinets or in rooms that can be locked.

    3) Locate photocopiers, printers, and fax machines to minimize access by visitors and unauthorized persons to confidential data and information.

    4) Make sure that directors and other management or supervisory personnel are familiar with and enforce security and confidentiality policies to ensure the security and confidentiality of the HMIS database and of Client information.

    5) Require and encourage the Participant staff to report security breaches and misuse of the HMIS database system.

    6) Encourage Clients to report any breaches of confidentiality that they observe in the Participant.

    7) Maintain the necessary software and updates on the Participant's computer systems to prevent viruses, worms, and unauthorized access to the Participant's computer systems and networks that could compromise the integrity of the HMIS system.

6. HUD HMIS – Privacy and Security Standards

   a. If required by one or more funding agreements, Participant shall review and comply with all standards for privacy and security in the Health Insurance Portability and Accountability Act (HIPAA) of 1996. If Participant is not required to comply with HIPAA standards, then Participant shall comply with all standards for privacy and security as set forth in the Department of Housing and Urban Development Homeless Management Information System (HMIS), Data and Technical Standards Final Notice, as found in the Federal Register dated July 30, 2004 Volume 69, Number 146.

   b. All Participants are required to submit a copy of their privacy notices to DHS for review and confirmation that each is in compliance with HUD requirements. Participants shall use common consent forms.

   c. Participants agree that the Participant is solely responsible for making sure their notices, forms, and other HMIS documentation meets HUD standards. Participants shall not rely upon DHS's review and shall indemnify and hold DHS, its staff, officers, members, and affiliates harmless from and against any and all claims for damages, losses, liabilities, costs, and/or reasonable expenses related to privacy and confidentiality issues and HUD requirements related to the HMIS database under this Agreement.

7. Reports

   a. Participant Reports

      1) The Participant may use the HMIS to report on identifying and statistical data on the Clients it serves, subject to the terms of this Agreement regarding Client confidentiality and applicable laws and regulations.

      2) The Participant may not use the HMIS to report on identifying and statistical data on Clients it does not serve.

   b. Aggregate Reports

      1) The Participant may make aggregate data available to other entities outside the system for funding or planning purposes pertaining to providing services to homeless persons. However, such aggregate data shall not contain information that could be used to personally identify individual Clients.

      2) Participants shall use only aggregate HMIS data that does not contain information that could be used to personally identify individual Clients for homeless policy and planning activities in preparing federal, state, or local applications for homelessness funding, to demonstrate the need for and effectiveness of programs and to obtain a system-wide view of program utilization in the State.

8. Termination

   a. DHS may terminate this Agreement for cause upon five (5) days written notice if it determines that the Participant has violated any material term of this Agreement. The Participant may appeal this decision to the HMIS Policy Committee at the next scheduled meeting of that committee.

b. This Agreement may be terminated by either party without cause upon thirty (30) days written notice.

c. Upon termination of this Agreement, the Participant shall cease using the HMIS Program, and shall return to DHS or destroy all confidential information received by Participant from the HMIS Program and all information created by the Participant on behalf of the HMIS Program. This provision shall apply to protected information that is in the possession of subcontractors or agents of the Participant. The Participant shall retain no documents containing private, protected health information. Notwithstanding the foregoing, the Participant may retain any document constituting the Participant's own business records, provided that those business records contain only information that would have been collected by Participant even if Participant had not participated in the HMIS Program.

d. In the event that the Participant determines that returning or destroying the protected information is infeasible, the Participant shall notify the HMIS Administrator of the conditions that make return or destruction infeasible within five (5) business days of termination. Upon notification that the return or destruction of the protected information is infeasible, the Participant shall continue to keep the protected information confidential as required by this Agreement and applicable laws and regulations, and shall limit further uses and disclosures of the information to those purposes that make the return or destruction infeasible.

9. Assignability. Participant may not assign this Agreement or any of its obligations hereunder without the prior written consent of DHS.

10. Modifications. Any modifications to this Agreement shall be in writing and agreed upon by DHS and Participants.

11. Availability of Funding. Participant understands and agrees that DHS's obligations under this Agreement are contingent upon DHS receiving McKinney-Vento funding from the US Department of Housing and Urban Development (HUD). DHS's obligations hereunder shall cease immediately without liability to DHS if such funding is no longer available.

12. Participant's Representations and Warranties. Participant represents and warrants as follows:

a. It has all necessary power and authority to enter this Agreement and to perform all of its obligations hereunder, and to manage, control, and ensure that each individual or entity that Participant authorizes, permits or allows to access the HMIS (or related services and equipment or facilities) also complies with the terms of this Agreement.

b. This Agreement has been duly and validly authorized, executed, and delivered by Participant and constitutes its valid and binding obligation.

c. In performing its obligations hereunder, Participant shall comply with all laws, rules, and regulations of all governmental bodies having jurisdiction.

d. Participant holds all required regulatory authorizations to perform this Agreement according to its terms.

e. Participant's obligations under this Agreement do not conflict with any other agreement.

13. DHS's Representations and Warranties. DHS represents and warrants as follows:

a. DHS has all the necessary power and authority to enter this Agreement and to perform all of its obligations hereunder.
b. This Agreement has been duly and validly authorized, executed, and delivered by DHS and constitutes its valid and binding obligation.
c. In performing its obligations hereunder, DHS shall comply with all laws, rules, and regulations or all governmental bodies having jurisdiction.
d. DHS holds all required regulatory authorizations and permits to provide the Services identified herein.
e. DHS obligations under this Agreement do not conflict with any other agreement.

14. Term: Unless otherwise terminated per Article 7 (Termination), this Agreement shall be in effect from July 1, 2024 to July 1, 2025. Any extensions shall be executed in writing by all parties.

15. Choice of Laws. This Agreement is governed by the laws of the State of California, and where applicable, to the HMIS, federal laws, and federal regulations.

16. Captions. Captions in this Agreement are provided for convenience of reference only and do not define, describe, or limit the scope or intent of this Agreement or any of the terms of this Agreement.

17. Entire Agreement. This Agreement contains the entire agreement between DHS and the Participant, collectively the Parties, and supersedes all prior or contemporaneous agreements, understandings, representations, and statements, oral or written, between the Parties with respect to the subject matter of this Agreement and the transactions contemplated by this Agreement.

18. Successors and Assigns. All terms of this Agreement shall be binding upon, inure to the benefit of, and be enforceable by the Parties and their respective legal representatives, successors, and assigns.

19. Further Assurances. The Parties shall cooperate with each other and execute any documents reasonably necessary to carry out the intent and purpose of this Agreement.

20. Severability. If any provision of this Agreement is declared or found to be illegal, unenforceable, or void by a court of competent jurisdiction, the provision shall in no way affect any other provision, covenant, or condition of this Agreement.

21. Authorizing the Action. This Agreement shall become effective, and an HMIS account established for the Participant, only upon the occurrence of both: (a) the execution of this document by an authorized representative of the Participant, and (b) the execution of this Agreement by the Director of DHS, or designee.

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

PARTICIPANT:

Participant Director Name, Title	Dated
Participant Name Street Address City, State, Zip Email: Phone: Mailing Address (if different from Street Address) City, State, Zip	Dated

COUNTY OF SONOMA:
Approved; Certificates 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 (If Applicable)	Dated

Approved as to Substance:

Privacy & Security Officer or Designee	Dated

Exhibit A. Privacy and Security of Personal and Personally Identifiable Information

(Tasseff Privacy Verson No. 6 Version 2024 May 15)

1. Recitals

   a. The Department of Housing and Urban Development (HUD) requires user of the Homeless Management Information System (HMIS) to implement safeguards designed to protect the personal information (PI) and personally identifiable information (PII) that the user maintains. To support that effort, HUD adopted regulations similar to the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In addition to complying with HUD regulations, contractors and subcontractors are obligated to protect all other PI, PII, or Sensitive PII (hereinafter identified as Protected Information) obtained on behalf of the County pursuant to this agreement consistent with the California Information Practices Act of 1977 (California Civil Code §§ 1798 et seq.).

   b. The purpose of this Exhibit is to set forth Contractor's privacy and security obligations with respect to Protected Information that Contractor may create, receive, maintain, use, or disclose on behalf of County pursuant to this Agreement.

   c. The terms used in this Exhibit, 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 consistent with such language as in effect or as amended.

   d. The provisions of this exhibit are supplemental to provisions of the Continuum of Care HMIS Participation Agreement. Contractor must comply with both the Participation agreement and this exhibit. Any conflicts in the language of the agreements shall favor the provision that protects the data better, mitigates vulnerabilities and incidents better, and/or more fully reports breaches.

2. Definitions

   a. "Breach" shall have the meaning given to such term under in HIPAA 45 CFR § 164.402 – Definitions.

   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. "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.

   d. "Personally Identifiable Information" (PII) refers to information that can be used to distinguish or trace an individual's identity, such as name, social security number, and biometric records; individually or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

      Some examples of PII include name, date of birth (DOB), email address, mailing address, medical history, family relationships, vehicle identifiers including license

plates, unique names, certificate, license, telephone and/or other specific reference numbers and/or any information that can directly identify an individual.

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

f. "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.

g. "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.

h. "Sensitive Personally Identifiable Information" (SPII) is PII that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone data elements.

Some examples of SPII include biometric information (e.g., DNA, iris images, fingerprint, and photographic facial images), Social Security Number (SSN), account numbers, and any other unique identifying number (e.g., Federal Housing Administration [FHA] case number, driver's license number, or financial account number, etc.). Other data elements such as citizenship or immigration status; medical information; ethnic, religious, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also SPII.

3. Terms of Agreement

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

Except as otherwise indicated in this Exhibit, Contractor may use or disclose Protected Information 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 this agreement.

b. Responsibilities of Contractor

Contractor agrees:

i. Safeguards. To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of Protected Information, to protect against anticipated threats or hazards to the security or integrity of Protected Information, and to prevent use or disclosure of Protected Information 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 this Exhibit. Contractor will provide County with its current policies upon request.

ii. General Privacy Controls. Not to use or disclose Protected Information other than as permitted or required by this Agreement or as required by applicable state and federal law.

1. The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure any Protected Information.
2. The Contractor and its employees, agents, or subcontractors shall not use any Protected Information for any purpose other than carrying out the Contractor's obligations under this Agreement.
3. The Contractor shall not disclose any Protected Information to anyone other than County except as permitted by this Agreement, authorized by the person who is the subject of Protected Information, or permitted by state and/or federal regulation.

iii. General Security Controls. Contractor and its sub-contractors or vendors shall take all steps necessary to ensure the continuous security of all computerized data systems containing Protected Information, and to protect paper documents containing Protected Information. These steps shall include, at a minimum:

1. Complying with and ensuring its sub-contractors or vendors comply with all the data system security precautions listed in this Exhibit including all documents incorporated by reference; and,
2. As applicable for the Contractor's information systems, 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
3. Preserving and ensuring its sub-contractors or vendors preserve, the confidentiality, integrity, and availability of Protected Information with administrative, technical and physical measures that conform to generally recognized industry standards and best practices that contractor 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-contractors or vendors. Contractor agrees to, and shall ensure that its sub-contractors or venders, comply with County's current and future information security policies, standards, procedures, and guidelines.

iv. Personnel Controls. Contractor shall implement the following personnel controls.

1. Employee Training. All workforce members who assist in the performance of functions or activities on behalf of the County, or access or disclose Protected Information must complete information privacy and security training, at least annually, at Contractor's expense. Training shall emphasize the high level of sensitivity and protection of Sensitive Personally Identifiable Information. 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.

2. 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.

3. 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.

4. 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.

v. System Security Review. Contractor must ensure audit control mechanisms that record and examine system activity are in place. Contractor must conduct and document a system risk assessment/security review on all systems processing and/or storing County PHI or PI. The assessment/security review must be performed a minimum of every two years, must review whether administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection, must identify system security risks, and must document risk findings. Reviews should include vulnerability scanning tools.

vi. Mitigation of Harmful Effects. To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Protected Information by Contractor or its subcontractors in violation of this Exhibit.

vii. Contractor's Agents and Subcontractors. To impose the same restrictions and conditions set forth in this Exhibit on any subcontractors or other agents with whom Contractor subcontracts any activities under this Agreement that involve the disclosure of Protected Information to the subcontractor.

viii. Cooperation with County. With respect to Protected Information, to cooperate with and assist the County to the extent necessary to ensure the County's compliance with the applicable terms of HUD regulations and the California Information Protection Act.

ix. Designation of an Individual Responsible Privacy and for Security

1. Contractor shall designate an individual to oversee its data security program who shall be responsible for carrying out the information security requirements of this Special Terms and Conditions document.

2. Contractor shall designate an individual to oversee its information privacy program who shall be responsible for carrying out the information privacy requirements of this Special Terms and Conditions document.

3. 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.

x. Privacy & Security 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 privacy & security audit. This is to ensure that Contractor's information privacy and security practices comply with contractual obligations, this Exhibit, and related state and federal regulations. Contractor shall ensure that its sub-contractors or vendors comply with these same requirements.

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

xii. Confidentiality of Alcohol and Drug Abuse Patient Records. Contractor agrees to comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2. Contractor is aware that criminal penalties may be imposed for a violation of these confidentiality requirements. All information subject to 42 CFR Part 2 shall be considered Sensitive Personally Identifiable Information.

c. Data Security Requirements

Contractor agrees to implement the following:

i. 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.

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

iii. 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.

iv. 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.

v. Data Destruction. If Protected Information is stored on a local device or server, when no longer needed, all Protected Information 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.

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.

vi. 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.

vii. 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.

viii. 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.

d. Paper Document Controls

i. 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.

ii. 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.

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

iv. 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.

v. 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.

vi. 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.

e. 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:

i. 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 Protected Information in electronic media or in any other media if the Protected Information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon discovery of a suspected security incident involving Protected Information. (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 Protected Information in violation of this Agreement or this Exhibit, 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.

Notice shall be provided to the County Privacy and Security Officer by calling (707) 565-4703, and emailing DHS-Privacy&Security@sonoma-county.org.

ii. Prompt Action. Upon discovery of a breach or suspected security incident, intrusion, or unauthorized access, use, or disclosure of County PHI, Contractor shall take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment. Contractor shall also take any action required by applicable Federal and State laws and regulations.

iii. Initial Investigation and Investigation Report. Contractor shall immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use, or disclosure of PHI within 24 hours of the discovery. Contractor shall submit a report to the County containing all relevant information known at the time.

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 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 provided in the Initial Report or Complete Report, 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 Complete Report is submitted The County will review and approve the determination of whether a breach occurred, whether individual notifications are required, and the Contractor's corrective action plan.

iv. Responsibility for Reporting of Breaches. If the cause of a breach of Protected Information 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 California SIMM 5340-C (https://cdt.ca.gov/wp-content/uploads/2021/02/SIMM_5340-C-1.pdf). 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.

v. 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 County Privacy Officer
1450 Neotomas Avenue, Suite 200
Santa Rosa CA 95405
Office: 707-565-4703
Message: 707-565-5703
Email: DHS-Privacy&Security@Sonoma-County.org

Exhibit B. County's Insurance Requirements

(Template 5 – Rev 2024 May 20)

With respect to performance of work under this Agreement, Contractor shall maintain and shall require all of its subcontractors, consultants, and other agents to maintain insurance as described below unless such insurance has been expressly waived by the attachment of a Waiver of Insurance Requirements. Any requirement for insurance to be maintained after completion of the work shall survive this Agreement.

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 Contractor 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 Employers Liability Insurance
    a. Required if Contractor has employees as defined by the Labor Code of the State of California.
    b. Workers Compensation insurance with statutory limits as required by the Labor Code of the State of California.
    c. Employers Liability with minimum limits of $1,000,000 per Accident; $1,000,000 Disease per employee; $1,000,000 Disease per policy.
    d. Required Evidence of Insurance: Certificate of Insurance.

If Contractor currently has no employees as defined by the Labor Code of the State of California, Contractor agrees to obtain the above-specified Workers Compensation and Employers Liability insurance should employees be engaged during the term of this Agreement or any extensions of the term.

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 Excess or Commercial Umbrella Liability Insurance. If Contractor maintains higher limits than the specified minimum limits, County requires and shall be entitled to coverage for the higher limits maintained by Contractor.
    c. Any deductible or self-insured retention shall be shown on the Certificate of Insurance. If the deductible or self-insured retention exceeds $100,000, it must be approved in advance by County. Contractor is responsible for any deductible or self insured retention and shall fund it upon County's written request, regardless of whether Contractor 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 endorsed as additional insureds for liability arising out of operations by or on behalf of the Contractor in the performance of this Agreement.

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 the additional insureds and Contractor and include a "separation of insureds" or "severability" clause which treats each insured separately.

h. Required Evidence of Insurance: Certificate of Insurance.

3. Automobile Liability Insurance

a. Minimum Limit: $1,000,000 combined single limit per accident. The required limits may be provided by a combination of Automobile Liability Insurance and Commercial Excess or Commercial Umbrella Liability Insurance.

b. Insurance shall cover all owned autos. If Contractor currently owns no autos, Contractor agrees to obtain such insurance should any autos be acquired during the term of this Agreement or any extensions of the term.

c. Insurance shall cover hired and non-owned autos.

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 $100,000, 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. Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.

e. Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

5. Cyber Liability Insurance – Network Security & Privacy Liability Insurance

a. Minimum Limit: $2,000,000 per claim or per occurrence, $2,000,000.00 aggregate.

b. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Contractor in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs (including notification costs), regulatory fines and penalties as well as credit monitoring expenses.

c. If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.

d. Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.

e. Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

6. Cyber Liability Insurance – Technology Errors and Omissions Insurance

a. Minimum Limit: $2,000,000 per claim or per occurrence, $2,000,000.00 aggregate.

b. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Contractor in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs (including notification costs), regulatory fines and penalties as well as credit monitoring expenses.

c. The Policy shall include, or be endorsed to include, property damage liability coverage for damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of the County in the care, custody, or control of the Contractor. If the Contractor maintains broader coverage and/or higher limits than the minimums shown above, the Entity requires and shall be entitled to the broader coverage and/or the higher limits maintained by the contractor. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to the Entity.

d. If the insurance is on a Claims-Made basis, the retroactive date shall be no later than the commencement of the work.

e. Coverage applicable to the work performed under this Agreement shall be continued for two (2) years after completion of the work. Such continuation coverage may be provided by one of the following: (1) renewal of the existing policy; (2) an extended

reporting period endorsement; or (3) replacement insurance with a retroactive date no later than the commencement of the work under this Agreement.

f. Required Evidence of Insurance: Certificate of Insurance specifying the limits and the claims-made retroactive date.

7. 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.

8. Documentation

a. All required Evidence of Insurance shall be submitted prior to the execution of this Agreement. Contractor agrees to maintain current Evidence of Insurance on file with County for the entire term of this Agreement and any additional periods if specified in Sections 1 – 4 above.

b. The name and address for Additional Insured endorsements and Certificates of Insurance is:

County of Sonoma, its Officers, Agents, and Employees
Attn: DHS – Contract & Board Item Development Unit
1450 Neotomas Avenue, Suite 200
Santa Rosa CA 95405
Email: 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 ten (10) days before expiration or other termination of the existing policy.

d. Contractor 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 thirty (30) days.

9. Policy Obligations

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

10. Material Breach

If Contractor fails to maintain insurance which is required pursuant to this Agreement, it shall be deemed a material breach of this Agreement. County, at its sole option, may terminate this Agreement and obtain damages from Contractor resulting from said breach. Alternatively, County may purchase the required insurance, and without further notice to Contractor, County may deduct from sums due to Contractor any premium costs advanced by County for such insurance. These remedies shall be in addition to any other remedies available to County.