Privacy and Security of Personal and Personally Identifiable Information

DHS Privacy & Security STC - #6 (Applies to HMIS Participating Agency Contractors)

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:

1) **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.

2) **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.

   a) The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure any Protected Information.

   b) 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.

   c) 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.

3) **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:

   a) 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,

   b) 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,

c) 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.

4) Personnel Controls. Contractor shall implement the following personnel controls.

a) **Employee Training**. All workforce members who assist in the performance of functions or activities on behalf of the County, or access or disclose 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.

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

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

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

5) **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.

6) **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.

7) **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.

8) **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.

9) **Designation of an Individual Responsible Privacy and for Security**

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

10) **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.

11) **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.

12) **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:

1) **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.

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

3) **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.

4) **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.

5) **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.

6) **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.

7) **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.

8) **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.

9) **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**

1) **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.

2) **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.

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

4) **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.

5) **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.

6) **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:

1) **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.

2) **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.

3) **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.

4) **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.

5) **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.

6) **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 Ave. Suite 200, Santa Rosa, CA 95405
Office: 707-565-4703
Message: 707-565-5703
Email: DHS-Privacy&Security@Sonoma-County.org