COUNTY OF TULARE
EXHIBIT F
TO HHSA SERVICES AGREEMENT
INFORMATION CONFIDENTIALITY AND SECURITY REQUIREMENTS
(Form revision approved 09/23/2019)

I. Definitions. For purposes of this Exhibit, the following definitions shall apply:

A. Public Information: Information that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.

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

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

D. Personal Information: Personal Information includes the following:

1. Specific items of personal information (name plus Social Security number, driver license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person.

2. For purposes of this provision, identity shall include, but not be limited to name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph. See Civil Code sections 1798.29 and 1798.82.

3. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request

E. Nondisclosure. The CONTRACTOR and its employees, agents, or subcontractors shall protect from unauthorized disclosure any Personal Information, Sensitive Information, or Confidential Information (hereinafter identified as PSCI).

II. The CONTRACTOR and its employees, agents, or subcontractors shall not use any PSCI for any purpose other than carrying out the CONTRACTOR's obligations under this Agreement.

III. The CONTRACTOR and its employees, agents, or subcontractors shall promptly transmit to the COUNTY all requests for disclosure of any PSCI not emanating from the person who is the subject of PSCI.

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

V. The CONTRACTOR shall observe the following requirements:

A. Safeguards. The CONTRACTOR shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PSCI, including electronic PSCI that it creates, receives, maintains, uses, or transmits on behalf of COUNTY. CONTRACTOR shall develop and maintain a written

B. information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the CONTRACTOR’s operations and the nature and scope of its activities, Including at a minimum the following safeguards:

COUNTY OF TULARE
EXHIBIT F
TO HHSA SERVICES AGREEMENT
INFORMATION CONFIDENTIALITY AND SECURITY REQUIREMENTS
(Form revision approved 09/23/2019)

1. Personnel Controls

a. ***Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of the COUNTY, or access or disclose COUNTY PSCI, must complete information Privacy and security training, at least annually. 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 contract termination.

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 DHCS inspection for a period of six (6) years following contract termination.

d. ***Background Check.*** Before a member of the workforce may access COUNTY PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The CONTRACTOR shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

2. Technical Security Controls

a. ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store COUNTY PHI or PI 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 COUNTY.

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

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

d. ***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.

e. ***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.

f. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing COUNTY PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not

to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

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

g. ***Data Destruction.*** When no longer needed, all COUNTY PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 8 0 0 - 88. Other methods require prior written permission of COUNTY.

h. ***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 1 0 minutes of inactivity.

i. ***Network and/or Operating System Warning Banners.*** All systems providing access to C O U N T Y PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

j. ***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.

k. ***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 PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.

3. Audit Controls

a. ***System Security Review.*** All systems processing and/or storing COUNTY PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection.

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

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

4. Business Continuity/Disaster Recovery Controls

a. Emergency Mode Operation Plan. CONTRACTOR must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic COUNTY PHI or PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

5. Paper Document Controls

a. ***Supervision of Data*****.** COUNTY PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. COUNTY PHI or PI in paper form shall not be left unattended at any

time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

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

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

d. ***Removal of Data*****.** COUNTY PHI or PI must not be removed from the premises of the CONTRACTOR except with express written permission of COUNTY.

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

f. ***Mailing*****.** Mailings of COUNTY PHI or PI shall be sealed and secured from damage or inappropriate viewing of 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 COUNTY to use another method is obtained.

C. Security Officer. The CONTRACTOR shall designate a Security Officer to oversee its data security program who will be responsible for carrying out its privacy and security programs and for communicating on security matters with COUNTY.

D. Discovery and Notification of Breach. The CONTRACTOR shall notify COUNTY **immediately by telephone call plus email or fax** upon the discovery of breach of security of PSCI in computerized form if the PSCI was, or is reasonably believed to have been, acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to COUNTY by the Social Security Administration **or within twenty-four (24) hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized use or disclosure of PSCI in violation of this Agreement, or potential loss of confidential data affecting this Agreement. CONTRACTOR shall take:

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

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

E. Investigation of Breach. The CONTRACTOR shall immediately investigate such security incident, breach, or unauthorized use or disclosure of PSCI and within seventy-two (72) hours of the discovery.

F. Written Report. The Contractor shall provide a written report of the investigation to the COUNTY HHSA Privacy & Compliance Officer ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.

G. Notification of Individuals. The CONTRACTOR shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The COUNTY HHSA Privacy & Compliance Officer shall approve the time, manner and content of any such notifications.

VI. Affect on lower tier transactions. The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, regardless of

whether they are for the acquisition of services, goods, or commodities. The CONTRACTOR shall incorporate the contents of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

VII. Contact Information. To direct communications to the above referenced COUNTY staff, the CONTRACTOR shall initiate contact as indicated herein. 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 Exhibit or the Agreement to which it is incorporated.

Tulare County HHSA Privacy & Compliance Officer
Tulare County HHSA 5957 S Mooney Blvd., Visalia, CA 93277 Email: complianceofficer@tularehhsa.org Telephone: (559) 624-7438

VIII. Audits and Inspections. From time to time, COUNTY may inspect the facilities, systems, books and records of the CONTRACTOR to monitor compliance with the safeguards required in the Information Confidentiality and Security Requirements (ICSR) exhibit. CONTRACTOR shall promptly remedy any violation of any provision of this ICSR exhibit. The fact that COUNTY inspects, or fails to inspect, or has the right to inspect, CONTRACTOR's facilities, systems and procedures does not relieve CONTRACTOR of its responsibility to comply with this ICSR exhibit.