COUNTY OF YUBA
REQUEST FOR PROPOSAL

Media Destruction

PROPOSAL CLOSING DATE:

Thursday, November 22, 2012
at 5:00pm PST

The County of Yuba is requesting proposals from qualified firms to provide media destruction services. Typically media will be hard drives but may also include RAM, phones, mobile phones, mobile computing devices, networking equipment and others. The services are to be provided on an "as-needed", "where-needed" basis. The County of Yuba currently has approximately 300 hard drives from personal PCs, laptops, copiers, and servers.

I. SCOPE OF WORK

a. All pricing must include travel and transportation charges and include itemized costs for services, including discounts available for specific volume levels.

b. All work performed must include a certificate of destruction, itemized to include serial numbers destroyed.

c. Hard drives must have data destroyed on-site either by shredding, degaussing, or rupturing the device. Proposals must indicate the method and process used.

d. Physical destruction can be done on-site or at the Contractor's business location. Pricing should be clearly listed for the type of service you are proposing. Physical destruction may include shredding, disintegrating, pulverizing, or incinerating as described in NIST special publication 800-88 Guidelines for Media Sanitation September 2006. Our preferred method is on-site shredding. Proposals for alternative options will be considered.

e. The bid price should include all options indicated above and shall include full compensation for furnishing all labor, materials, tools, equipment, plans, travel and incidentals for doing all work involved to provide such service.

f. A specification sheet(s) should be included with your proposal that indicates a detailed description of the destruction process in addition to all the services your company provides.

g. All hard drives must be destroyed in accordance with Federal Information Processing Standards (FIPS) 200 and Guidelines for Media Sanitation (NIST) SP 800-88.

h. The final contract will be performed on a work order request basis. A quote will be requested before scheduling a pick up. Once this work order request is signed by both parties, the hard drive pick-up can be scheduled.

II. STATEMENT OF QUALIFICATIONS

All submissions should include the following information:

- The name and location of your company
- The location of the office that will be servicing the County
- A company profile outlining its history, experience, size, and affiliations.
- The number of years the company has been in business

- An outline of a minimum of three current customers/clients with similar projects in scope and size, relevant volume statistics and the customers contact information
- Full disclosure of any data breaches encountered by your organization. Information to be provided shall include the scope of the breach, why/how it occurred and how any issues were resolved
- Process of how employees are selected and screened prior to and during employment that ensures appropriate clearances for handling sensitive data. Including but not limited to background checks (FBI and DOJ), DMV records, and so forth.

III. TECHNICAL PROPOSALS

Proposals must include a written response to the Scope of Work that demonstrates the Contractor's capabilities and experience in providing the required services. The technical proposal should include the Contractor's process from receipt to final disposal.

IV. ADDITIONAL REQUIREMENTS

a. Contractor must have direct experience conducting work in similar scope and implementation on at least three projects of equal or greater scope.

b. Contractor shall designate one person or representative of the Contractor who is authorized to act on its behalf with respect to this specified work.

c. The Contractor must demonstrate they have the technical expertise, experience, facilities, capabilities, and financial resources necessary to perform the work in a satisfactory manner.

d. Part of the selection process will include a credit check and financial evaluation of the business.

e. Selection will be made by a County Evaluation Team. The Evaluation Team may deem it necessary to schedule presentations and/or interview applicants and key personnel. The County retains the right to interview applicants as part of the selection process. Members of the Evaluation Team are not to be contacted by the proposers.

f. All work performed shall be in compliance with appropriate OSHA and Hazardous Waste Handling standards, as well as all Federal, State, County, and local ordinances and regulations. Contractor must obtain all licenses and permits required and Contractor shall bear the cost for meeting this standard for all employees.

g. All work performed and completed under the resulting agreement is subject to the acceptance of the County or its authorized representative.

h. Contractor should be able to provide proof that they have all appropriate state, federal, and local licenses required for the completion of this project, without any delinquencies.

i. Contractor should be able to provide proof of continuous General Liability, Auto and Workers Compensation Insurance coverage for the last five years.

j. Contractor shall furnish to the County, *upon award of contract,* certificate of insurance naming the County as an additional insured party in amounts requested by County and maintain such insurance during term of contract.

V. EVALUATION CRITERIA

The County reserves the right to cancel this Request for Proposal for any reason without any liability to any Contractor or to waive irregularities at its discretion. This solicitation does not constitute a contract offer of employment, or offer of purchase. The County may select any Option or combination of Options outlined in the scope of work at its own discretion. The County makes no representation that any contract will be awarded to any respondent to this solicitation. The County also reserves the right to reject any and all proposals at its sole discretion.

The contract(s), if awarded, will be awarded to the Contractor whose proposal is considered the best value to the County. Best value will be determined based on price, responsiveness, and responsibility:

a. The lowest price is determined by the total cost to the County.

b. Responsiveness means a Contractor who has submitted a proposal that conforms to the solicitation documents in all material aspects.

c. A responsible Contractor and/or Consultant shall mean a Contractor and/or Consultant who has the capability, in all respects, to fully perform the contract requirements and the moral and business integrity and reliability that will assure good faith performance. Qualifications, interview, experience, and financial stability may all be taken into consideration.

Thus the result will not be determined based solely on price. Although price is a factor, the County will consider awarding the contract(s) to the Contractor that meets the best interest of the County as interpreted by the County.

The County reserves the right to negotiate the terms of the final contract agreement. The final determination of equipment, services, and dates and time work to be conducted will be provided and incorporated into the final agreement for services (contract).

VI. PROPOSAL SUBMITTALS

Please include the following with your proposal in this order:

- Technical Proposal
- Statement of Qualifications
- Proof of Insurance Coverages
- Attached Proposal Forms (2 pages)
- Workers Compensation History (letter from provider is sufficient)
- Key Contact Person Information

VII. TERMS AND CONDITIONS

Proposals are subject to the following terms and conditions:

a. **Contract Term.** The term of the agreement resulting from this solicitation will be for the period of one year, with the option for two-one year extensions.

b. **Project Schedule.** Upon receipt of proposals, and suitable review, County expects to select a Contractor. Once selected, Contractor and County will complete contract and agree upon start date and work schedule. County desires for the project to begin in January 2013.

c. **Contract Form.** The final contract(s) will incorporate the appropriate terms and conditions from this solicitation. Attached Exhibit A and B are samples of our Confidentiality Provisions Agreement and HIPAA Business Associate Agreement. Each of these will be part of the final contract.

d. **References.** To receive consideration, proposals must clearly and specifically address how the requirements for each item will be met. Proposal must include a Statement of Experience and three references including contact information from projects similar to ours which we may contact as references.

e. **Submittal Instructions.** Before submitting a proposal, Contractor shall fully inform themselves as to all conditions and limitations and shall include in the proposal a sum to cover the cost of all items. TWO copies of the contractor's proposals must be submitted in a sealed envelope, clearly marked ***"Media Destruction"*** to:

   Yuba County Department of Administrative Services
   Attn: Purchasing and Contracts
   915 Eighth Street, Suite 119
   Marysville, California 95901

   No responsibility will attach to a County employee for the premature opening of a proposal not properly addressed and identified. Proposals will not be publicly opened and read. Proposals will be privately reviewed and evaluated by a County Evaluation Team.

f. **Proposal Due Date.** In order to be considered, proposals must be received at the above address no later than ***Thursday, November 22, 2012 at 5:00pm PST***. A proposal may be withdrawn by written request received from the County prior to the time set for the closing date.

g. **Proposal Validity.** Proposals for the Hard Drive Destruction must be valid for a period of not less than ninety days (90) after the solicitation closing date.

Contact Information. Andrea Armstrong, Contracts and Purchasing Administrator for Administrative Services, is the designated contact person for questions related to this Request for Proposal. All questions must be received in writing via email, fax, or USPS mail service. Responses

will be returned in writing and only the answers in writing will constitute an amendment as the correct, accurate and binding response from the County. All questions and responses will be posted and shared with all participants, applicants and Contractor/Consultants. Andrea's contact information is: email aarmstrong@co.yuba.ca.us, fax 530-749-7884. Andrea's contact phone number is 530-749-7880.

All questions must be received in writing by ***Friday, November 16, 2012*** and will be posted on at the County's webpage at:

http://www.co.yuba.ca.us/departments/admin%20services/purchasing%20solicitaions.aspx

Please check back to the website often for additional information, addendums, and responses to questions.

COUNTY OF YUBA
PRICE PROPOSAL FORM
Page 1 of 2

By signing below, I certify that I have read, understand and agree to all requirements of this request for proposal, all addenda issued and the contractual requirements as statement within the project documents. The undersigned has carefully checked all figures in his/her proposal and understands the County of Yuba will not be responsible for any errors or omissions in preparing this proposal. The proposal shall remain valid for any and all services provided for a period of sixty days.

RFP NAME: **MEDIA DESTRUCTION**

FIRM NAME: _____

CONTACT NAME: _____

ADDRESS OF FIRM: _____

_____

TELEPHONE: _____

EMAIL ADDRESS: _____

FEDERAL ID NUMBER: _____

DUNS NUMBER: _____

AUTHORIZED SIGNATURE: _____

NAME & TITLE: _____

ADDENDA ACKNOWLEDGEMENT

Addendum#	Initials

COUNTY OF YUBA
PRICE PROPOSAL FORM
Page 2 of 2

(1) Specify types of Media (e.g. Hard Drives, RAM, Phones, Mobile Devices, Networking Equipment, etc.)

(2) Quantity (please itemize discounts available at specific volume levels)

(1) Type of Media	(2) Quantity	On-Site (price each)	Total	Off-Site (price each)	Total
Example: Hard Drives	1-199	$5.99	$71.88	$0.00	$0.00
Example: Hard Drives	200-1000	$2.99	$35.88	$0.00	$0.00

All pricing must include travel and transportation charges and include itemized costs for the services including discounts available at specific volume levels

Quantities listed are approximates and are estimates based on past usage and are not to be construed as a commitment. No minimum or maximum is guaranteed or implied.

EXHIBIT A

CONFIDENTIALITY PROVISIONS AND STATEMENTS

1.0 INTRODUCTION

For the purposes of carrying out a contract for Professional Services entered into between the COUNTY OF YUBA (hereinafter "COUNTY") and <><> (hereinafter "CONTRACTOR"), the COUNTY has provided the CONTRACTOR access to Confidential Information. The provisions and statement sets forth in this document outline the CONTRACTOR's responsibilities for safeguarding this information.

2.0 DEFINITIONS.

2.1 CONFIDENTIAL INFORMATION shall include, but is not limited to, personally identifiable information, protected health information, financial information, financial account numbers, driver's license numbers, social security numbers, marital status, etc.

2.2 PERSONALLY IDENTIFIABLE INFORMATION is Confidential Information and includes, but is not limited to, names, dates of birth, social security numbers, addresses, phone numbers, driver's license numbers, State ID numbers, etc.

2.3 BREACH shall mean the acquisition, access, use or disclosure of Confidential Information which compromises the security or privacy of such information.

2.4 SECURITY INCIDENT shall mean any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any Confidential Information.

3.0 BACKGROUND.

The COUNTY maintains Confidential Information to perform functions, activities, and/or services directly related to the administration of a social service program. Such Confidential Information may not be used, accessed, or disclosed for any other purposes.

The COUNTY must take appropriate steps to ensure its compliance with all applicable state and federal confidentiality laws and desires to protect the privacy of those to which it provides services. As such, it must require that CONTRACTOR also obey all applicable state and federal laws. Any individual who violates the privacy, confidentiality, or security of Confidential Information in any form or medium may be subject to civil and/or criminal prosecution under state and federal law.

Establishing safeguards for Confidential Information can limit the potential exposure of Confidential Information and CONTRACTOR is expected to adhere to current industry standards and best practices in the management of data collected by, or on behalf of, the COUNTY, and within the CONTRACTOR's possession.

However, even with sound practices and safeguards, exposure can occur as a result of a theft, loss, compromise or Breach of the data and/or systems containing data. At these times, the CONTRACTOR must immediately report the incident surrounding the loss or Breach of data in the CONTRACTOR's possession and absorb any associated costs as deemed by the COUNTY to be reasonable and necessary.

4.0 PROVISIONS.

4.1 The CONTRACTOR shall sign the "Confidentiality Provisions and Statements" and adopt it by reference in the underlying Agreement.

4.2 The COUNTY requires at least the following minimum standards of care in handling the Confidential Information:

4.2.1 Securing all areas where Confidential Information is maintained and/or stored;

4.2.2 Utilizing all industry standard encryption and methodology through which Confidential Information is transmitted and/or stored. This includes desktop and laptop computers (whole drive encryption —not file encryption), personal digital assistants (PDA), smart phones, thumb or flash-type drives, CDs, diskettes, backup tapes, etc.;

4.2.3 Limiting the removal of Confidential Information from the CONTRACTOR's premises except for those purposes as designated in the underlying Agreement;

4.2.4 Ensuring only the minimum necessary amount of Confidential Information is downloaded and/or accessed when absolutely necessary for the purposes as designated in the underlying Agreement;

4.2.5 Not leaving Confidential Information unattended or accessible to unauthorized individuals; and

4.2.6 Disposing of Confidential Information, after obtaining COUNTY authorization and approval, through confidential means for the purposes designated in the underlying Agreement.

4.3 Confidential Information shall only be used or disclosed for the purposes designed in the underlying Agreement and at no time shall be disclosed or used for personal, non-contract/agreement related reasons, unless specifically authorized by the COUNTY.

4.4 In all circumstances, the CONTRACTOR shall have no ownership rights or interests in any data or information, including Confidential Information. All data collected by the CONTRACTOR on behalf of the COUNTY, or received by the CONTRACTOR on behalf of the COUNTY, is owned by the COUNTY. There are no exceptions to this provision.

4.5 The COUNTY may periodically monitor and/or audit use of the information systems and other record-keeping systems at a CONTRACTOR's location or COUNTY location in an effort to ensure compliance with these provisions.

4.6 If there is an incident involving theft, loss, compromise, and/or Breach of Confidential Information, the CONTRACTOR must notify the COUNTY immediately and under no circumstances no less than twenty four (24) hours after discovery of such an incident.

4.7 If the incident involves a theft or is incidental to another crime, the CONTRACTOR shall notify the appropriate law enforcement officials and a police report generated to document the circumstances of the incident so as to establish whether the crime involved a motive to obtain the Confidential Information. The police report will be forwarded to the COUNTY within forty eight (48) hours of receipt of the report.

4.8 NOTIFICATION OF BREACH.

4.8.1 Upon the suspicion or discovery of a Breach, Security Incident, intrusion, or unauthorized use or disclosure of Confidential Information, the CONTRACTOR shall notify the COUNTY within twenty four (24) hours by telephone in addition to follow up by either email or fax.

4.8.2 Notification of any Breach, Security Incident, or unauthorized access as described in section 4.8.1 shall be provided to:
Rick Gilmore, Information Security Officer
Phone: (530) 749-7880
Email: rgilmore@co.yuba.ca.us
Fax: (530) 749-7884

4.8.3 The CONTRACTOR shall immediately investigate such actual or suspected Breach, Security Incident, or unauthorized access of Confidential Information. Within seventy two (72) hours of the discovery, if an actual Breach has occurred, the CONTRACTOR shall notify the individual identified in section 4.8.2 of the following:

(a) What data elements were involved and the extent of the data involved in the Breach (e.g. number of records or affected individual's data);

(b) The identity of the unauthorized persons known or reasonably believed to have improperly used or disclosed Personally Identifiable Information (PII), Personal Health Information (PHI) and/or Confidential Information;

(c) A description of where the Confidential Information is believed to have been improperly transmitted, sent, or utilized;

(d) A description of the probable causes of the improper use or disclosure; and

(d) Whether any state or federal laws requiring individual notifications of breaches are triggered.

4.8.4 The COUNTY will coordinate with the CONTRACTOR to determine additional specific actions that will be required of the CONTRACTOR for mitigation of the Breach, which may include notification to the individual or other authorities.

4.8.5 All associated costs shall be borne by the CONTRACTOR. This may include, but is not limited to, costs associated with notifying the affected individuals.

4.9 The COUNTY may require that the CONTRACTOR provide evidence of adequate background checks for individuals who are entrusted by the CONTRACTOR to work with the COUNTY's Confidential Information.

4.10 The COUNTY requires that the CONTRACTOR have comprehensive policies and procedures to adequately safeguard the Confidential Information before it is conveyed to the CONTRACTOR. The CONTRACTOR's policies should articulate all safeguards in place for the COUNTY's Confidential Information, including provisions for destruction of all data and backup copies of data. All COUNTY-owned media containing Confidential Information shall be returned to the COUNTY when no longer legitimately needed by the CONTRACTOR.

5.0 ACKNOWLEDGEMENT OF RECEIPT AND SIGNATURE.

The CONTRACTOR hereby understands the above provisions and statements. The CONTRACTOR further understands the sensitivity of the Confidential Information and understands that the CONTRACTOR must protect the confidentiality of all COUNTY information placed within the CONTRACTOR's care or which the CONTRACTOR may come across during the course of the Agreement.

DATED: _____

CONTRACTOR

[to be executed with contract]

_____
(Signature)
(Print Name and Title)

EXHIBIT B

HIPAA BUSINESS ASSOCIATE AGREEMENT

This Attachment shall constitute the Business Associate Agreement (the "Agreement") between CONTRACTORS NAME (the "Business Associate") and the County of Yuba (the "Covered Entity"), and applies to the functions Business Associate will perform on behalf of Covered Entity (collectively, "Services"), that are identified in the Master Agreement (as defined below).

1. **Purpose.** This Agreement is intended to ensure that the Business Associate will establish and implement appropriate privacy and security safeguards with respect to "Protected Health Information" (as defined below) that the Business Associate may receive in connection with the Services to be provided by the Business Associate to the Covered Entity's designated agent, and that such safeguards will be consistent with the standards set forth in regulations promulgated under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") as amended by the Health Information Technology for Economic and Clinical Health Act as set forth in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 ("HITECH Act").

2. **Regulatory References.** All references to regulatory Sections, Parts and Subparts in this Agreement are to Title 45 of the Code of Federal Regulations as in effect or as amended, and for which compliance is required, unless otherwise specified.

3. **Definitions.** Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms are defined in Sections 160.103, 164.304 and 164.501.

(a) Business Associate. "Business Associate" shall mean the party identified above as the "Business Associate".

(b) Breach. "Breach" shall have the same meaning as the term "breach" in Section 164.402.

(c) Covered Entity. "Covered Entity" shall mean the County of Yuba, a hybrid entity, and its designated covered components, which are subject to the Standards for Privacy and Security of Individually Identifiable Health Information set forth in Parts 160 and 164.

(d) Designated Record Set. "Designated Record Set" shall have the same meaning as the term "designated record set" in Section 164.501.

(e) Electronic Protected Health Information. "Electronic Protected Health Information" ("EPHI") is a subset of Protected Health Information and means individually identifiable health information that is transmitted or maintained in electronic media, limited to the information created, received, maintained or transmitted by Business Associate from or on behalf of Covered Entity.

(f) Individual. "Individual" shall have the same meaning as the term ''Individual'' in Section 164.501 and shall include a person who qualifies as a personal representative in accordance with Section 164.502(g).

(g) Master Agreement. "Master Agreement" shall mean the contract or other agreement to which this Attachment is attached and made a part of.

(h) Minimum Necessary. "Minimum Necessary" shall mean the minimum amount of Protected Health Information necessary for the intended purpose, as set forth at Section 164.514(d): *Standard: Minimum Necessary.*

(i) Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at Part 160 and Part 164, Subparts A and E.

(j) Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in Section 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(k) Required By Law. "Required by law" shall have the same meaning as the term "required by law" in Section 164.103.

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

(m) Security Incident. "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system, but does not include minor incidents that occur on a daily basis, such as scans, "pings", or unsuccessful random attempts to penetrate computer networks or servers maintained by Business Associate.

(n) Security Rule. "Security Rule" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.

(o) Unsecured Protected Health Information. "Unsecured Protected Health Information" shall have the same meaning as the term "unsecured protected health information" in Section 164.402, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

4. **Compliance with the HIPAA Privacy and Security Rules.**

(a) Business Associate acknowledges that it is required by Sections 13401 and 13404 of the HITECH Act to comply with the HIPAA Security Rule, Sections 164.308 through 164.316, and the use and disclosure provisions of the HIPAA Privacy Rule, Sections 164.502 and 164.504.

(b) Business Associate agrees not to use or further disclose Protected Health Information. No disclosures of Protected Health Information or other confidential information is permitted.

5. **Permitted Uses and Disclosures.**

(a) Business Associate may not use or disclose Protected Health Information in performance of functions, activities, or services for, or on behalf of, Covered Entity. No disclosures of Protected Health Information or other confidential information is permitted.

(b) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities consistent with Section 164.502(j).

6. **Appropriate Safeguards.**

(a) Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of Protected Health Information other than as provided for by this Agreement. Appropriate safeguards shall include implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Protected Health Information that is created, received, maintained or transmitted on behalf of the Covered Entity.

(b) To the extent practicable, Business Associate will secure all Protected Health Information by technological means that render such information unusable, unreadable, or indecipherable to unauthorized individuals and in accordance with any applicable standards or guidance issued by the Department of Health and Human Services under Section 13402 of the HITECH Act.

7. **Reporting Unauthorized Uses and Disclosures.**

(a) Business Associate agrees to notify Covered Entity of any breach, or security incident involving Unsecured Protected Health Information of which it becomes aware, including any access to, or use or disclosure of Protected Health Information. Such notification will be made within five (5) business days after discovery and will include, to the extent possible, the identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used or disclosed, a description of the Protected Health Information involved, the nature of the unauthorized access, use or disclosure, the date of occurrence, and a description of any remedial action taken or proposed to be taken by Business Associate. Business Associate will also provide to Covered Entity any other available information that the Covered Entity is required to include in its notification to the Individual under Section 164.404(c) at the time of the initial report or promptly thereafter as the information becomes available.

(b) In the event of a request by law enforcement under Section 164.412, Business Associate may delay notifying Covered Entity for the applicable timeframe.

(c) A breach or unauthorized access, use, or disclosure shall be treated as discovered by the Business Associate on the first day on which such unauthorized access, use, or disclosure is known, or should reasonably have been known, to the Business Associate or to any person, other than the individual committing the unauthorized disclosure, that is an employee, officer, subcontractor, agent or other representative of the Business Associate.

(d) In meeting its obligations under this section, it is understood that Business Associate is not acting as the Covered Entity's agent. In performance of the work, duties, and obligations and in the exercise of the rights granted under this Agreement, it is understood and agreed that Business Associate is at all times acting as an independent contractor in providing services pursuant to this Agreement and the Master Agreement.

8. **Mitigating the Effect of a Breach, Security Incident, or Unauthorized Access, Use or Disclosure of Unsecured Protected Health Information.**

(a) Business Associate agrees to mitigate, to the greatest extent possible, any harm that results from the breach, security incident, or unauthorized access, use or disclosure of Unsecured Protected Health Information by Business Associate or its employees, officers, subcontractors, agents, or other representatives.

(b) Following a breach, security incident, or any unauthorized access, use or disclosure of Unsecured Protected Health Information, Business Associate agrees to take any and all corrective action necessary to prevent recurrence, to document any such action, and to make said documentation available to Covered Entity.

(c) Except as required by law, Business Associate agrees that it will not inform any third party of a breach or unauthorized access, use or disclosure of Unsecured Protected Health Information without obtaining the Covered Entity's prior written consent. Covered Entity hereby reserves the sole right to determine whether and how such notice is to be provided to any Individuals, regulatory agencies, or others as may be required by law, regulation or contract terms, as well as the contents of such notice.

9. **Indemnification.**

(a) Business Associate agrees to hold harmless, defend at its own expense, and indemnify Covered Entity for the costs of any mitigation undertaken by Business Associate pursuant to Section 8, above.

(b) Business Associate agrees to assume responsibility for any and all costs associated with the Covered Entity's notification of Individuals affected by a breach or unauthorized access, use or disclosure by Business Associate or its employees, officers, subcontractors, agents or other representatives when such notification is required by any state or federal law or regulation, or under any applicable contract to which Covered Entity is a party.

(c) Business Associate agrees to hold harmless, defend at its own expense and indemnify Covered Entity and its respective employees, directors, officers, subcontractors, agents or other members of its workforce (each of the foregoing hereinafter referred to as "Indemnified Party") against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with any breach of this Agreement or from any acts or omissions related to this Agreement by Business Associate or its employees, directors, officers, subcontractors, agents or other members of its workforce. Accordingly, on demand, Business Associate shall reimburse any Indemnified Party for any and all actual and direct losses, liabilities, lost profits, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third party which results from the Business Associate's acts or omissions hereunder. Business Associate's obligation to indemnify any Indemnified Party shall survive the expiration or termination of this Agreement.

10. **Individuals' Rights.**

(a) Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner designated by the Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under Section 164.524.

(b) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to make pursuant to Section 164.526, at the request of Covered Entity or an Individual, and in the time and manner designated by the Covered Entity.

(c) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with Section 164.528.

(d) Business Associate agrees to provide to Covered Entity or an Individual, in the time and manner designated by Covered Entity, information collected in accordance with Section 10(c) of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with Section 164.528.

(e) Business Associate agrees to comply with any restriction to the use or disclosure of Protected Health Information that Covered Entity agrees to in accordance with Section 164.522.

11. **Obligations of Covered Entity.**

(a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with Section 164.520, as well as any changes to such notice.

(b) Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with Section 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

12. **Agents and Subcontractors of Business Associate.**

(a) Business Associate agrees they will not disclose Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees in writing to the same restrictions, conditions and requirements that apply through this Agreement to Business Associate with respect to such information, including the requirement to promptly notify the Business Associate of any instances of unauthorized access to or use or disclosure of Protected Health Information of which it becomes aware. Upon request, Business Associate shall provide copies of such agreements to Covered Entity.

(b) Business Associate shall implement and maintain sanctions against any agent, subcontractor or other representative that violates such restrictions, conditions or requirements and shall mitigate the effects of any such violation.

13. **Audit, Inspection, and Enforcement.**

(a) Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity, available to any state or federal agency, including the Secretary, for the purposes of determining compliance with HIPAA and any related regulations or official guidance.

(b) With reasonable notice, Covered Entity and its authorized agents or contractors may audit and/or examine Business Associate's facilities, systems, policies, procedures, and documentation relating to the security and privacy of Protected Health Information to determine compliance with the terms of this Agreement. Business Associate shall promptly correct any violation of this Agreement found by Covered Entity and shall certify in writing that the correction has been made. Covered Entity's failure to detect any unsatisfactory practice does not constitute acceptance of the practice or a waiver of Covered Entity's enforcement rights under this Agreement.

14. **Permissible Requests by Covered Entity**. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

15. **Term and Termination.**

(a) The terms of this Agreement shall remain in effect for the duration of all services provided by Business Associate under the Master Agreement and for so long as Business Associate remains in possession of any Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity unless Covered Entity has agreed in accordance with this section that it is not feasible to return or destroy all Protected Health Information.

(b) Upon termination of the Master Agreement, Business Associate shall recover any Protected Health Information relating to the Master Agreement and this Agreement in its possession and in the possession of its subcontractors, agents or representatives. Business Associate shall return to Covered Entity, or destroy with the consent of Covered Entity, all such Protected Health Information, in any form, in its possession and shall retain no copies. If Business Associate believes it is not feasible to return or destroy the Protected Health Information, Business Associate shall so notify Covered Entity in writing. The notification shall include: (1) a statement that the Business Associate has determined that it is not feasible to return or destroy the Protected Health Information in its possession, and (2) the specific reasons for such determination. If Covered Entity agrees in its sole discretion that Business Associate cannot feasibly return or

destroy the Protected Health Information, Business Associate shall ensure that any and all protections, requirements and restrictions contained in the Master Agreement and this Agreement shall be extended to any Protected Health Information for so long as Business Associate maintains such Protected Health Information, and that any further uses and/or disclosures will be limited to the purposes that make the return or destruction of the Protected Health Information infeasible.

(c) Covered entity may immediately terminate the Master Agreement if it determines that Business Associate has violated a material term of this Agreement.

16. **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity and Business Associate to comply with the requirements of the HIPAA Privacy and Security Rules and the HITECH Act.

17. **Entire Agreement.** This Attachment constitutes the entire HIPAA Business Associate Agreement between the parties, and supersedes any and all prior HIPAA Business Associate Agreements between them.

18. **Notices.**

(a) All notices required or authorized by this Agreement shall be in writing and shall be delivered in person or by deposit in the United States mail, by certified mail, postage prepaid, return receipt requested. Any notice sent by mail in the manner prescribed by this paragraph shall be deemed to have been received on the date noted on the return receipt or five days following the date of deposit, whichever is earlier.

(b) Any mailed notice, demand, request, consent, approval or communication that Covered Entity desires to give to Business Associate shall be addressed to Business Associate at the mailing address set forth in the Master Agreement.

(c) Any mailed notice, demand, request, consent, approval or communication that Business Associate desires to give to Covered Entity shall be addressed to Covered Entity at the following address:

Yuba County Privacy Officer
915 8th Street, Suite 119
Marysville, CA 95901

(d) For purposes of subparagraphs (b) and (c) above, either party may change its address by notifying the other party of the change of address.

19. **Lost Revenues; Penalties/Fines.**

(a) Lost Revenues. Business Associate shall make Covered Entity whole for any revenues lost arising from an act or omission in billing practices by Business Associate.

(b) Penalties/Fines for Failure to Comply with HIPAA. Business Associate shall pay any penalty or fine assessed against Covered Entity arising from Business Associate's failure to comply with the obligations imposed by HIPAA.

(c) Penalties/Fines (other). Business Associate shall pay any penalty or fine assessed against Covered Entity arising from Business Associate's failure to comply with all applicable Federal or State Health Care Program Requirements, including, but not limited to any penalties or fines which may be assessed under a Federal or State False Claims Act provision.

IN WITNESS WHEREOF, the parties hereto have executed this AGREEMENT as set forth below:

COUNTY
Yuba County

By:_____ On:_____
NAME, TITLE (of person signing contract) (Date)

CONTRACTOR
CONTRACTOR NAME

By:_____ On:_____
(Name), (Title) (Date)

APPROVED AS TO FORM:

_____
for Angil P. Morris-Jones
Yuba County Counsel

HIPAA BUSINESS ASSOCIATE PROVISIONS

EXHIBIT 1

As provided in Paragraph 5 of this Agreement, Business Associate may use Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity for the purposes specified below, or as otherwise specified in the Master Agreement authorizing functions, activities, or services for, or on behalf of, Covered Entity, provided that such use would not violate the Privacy Rule if done by Covered Entity. Business Associate may not disclose Protected Health Information other than pursuant to Section 5(b) of this Agreement.

Authorized Purposes:
Media Destruction, transportation, and disposal as provided in Contractor's scope of work.