

Internal Contract No: 354-158-M-E2009
Purchasing Contract No: 308-S1010
Index Code: 419100

CONTRACT ROUTING SHEET

Date Prepared: October 25, 2010

Need Date: 11/8/10

PROCESSING DEPARTMENT:
Department: Health Svcs Dept – MH Div.
Dept. Contact: Thomas Michaelson
Phone #: 6203
Department
Head Signature: *Neda West*
NWR Neda West, Director

CONTRACTOR:
Name: Clinicians Telemed Medical Group, Inc.
Address: 1801 16th Street, Suite B
Bakersfield, CA 93301
Phone: 661-326-8060

CONTRACTING DEPARTMENT: Health Services Department – Mental Health Division
Service Requested: Healthcare consultative, diagnostic and treatment planning services
Contract Term: Date of execution [redacted] to 6/30/11 Contract Value: \$58,500.00
Compliance with Human Resources requirements? Yes No
Compliance verified by: Chris Little

COUNTY COUNSEL: (Must approve all contracts and MOU's)
Approved: Disapproved: Date: Nov. 9, 2010 By: *R. Bonelli*
Approved: Disapproved: Date: 12/14/10 By: *[Signature]*
Approved: Disapproved: Date: Jan 13, 2011 By: *[Signature]*
Art IV, p. 10, Exhibits D-1 and D-2
made requested change to

PLEASE FORWARD TO RISK MANAGEMENT. THANKS!

RISK MANAGEMENT: (All contracts and MOU's except boilerplate grant funding agreements)
Approved: Disapproved: Date: 11/10/10 By: *[Signature]*
Approved: Disapproved: Date: _____ By: _____

OTHER APPROVAL: (Specify department(s) participating or directly affected by this contract).
Departments: _____
Approved: _____ Disapproved: _____ Date: _____ By: _____
Approved: _____ Disapproved: _____ Date: _____ By: _____

[Signature] 9/20/10 Program Mgr/Date
[Signature] 10/22/10 Finance/Date

AGREEMENT FOR SERVICES #354-158-M-E2009

THIS AGREEMENT made and entered into by and between the County of El Dorado, a political subdivision of the State of California (hereinafter referred to as "COUNTY") and Clinicians Telemed Medical Group, Inc., a California Corporation duly qualified to conduct business in the State of California, whose principal place of business is 1801 16th Street, Suite B, Bakersfield, CA 93301, (hereinafter referred to as "CONTRACTOR");

RECITALS

WHEREAS, COUNTY has determined that it is necessary to obtain a contractor to provide healthcare consultative, diagnostic and treatment planning services utilizing interactive audio, video and/or data communications; and

WHEREAS, CONTRACTOR has represented to COUNTY that it is specially trained, experienced, expert and competent to perform the special services required hereunder and COUNTY has determined to rely upon such representations; and

WHEREAS, it is the intent of the parties hereto that such services be in conformity with all applicable Federal, State and local laws; and

WHEREAS, COUNTY has determined that the provision of these services provided by CONTRACTOR is in the public's best interest, and that these services are more economically and feasibly performed by outside independent Contractors as well as authorized by the El Dorado County Charter, Section 210 (b) (6) and/or Government Code 31000;

NOW, THEREFORE, COUNTY and CONTRACTOR mutually agree as follows:

Article I. SCOPE OF SERVICES
Section 1.01 OBLIGATIONS OF CONTRACTOR

- (a) Physician Services During the term of this Agreement, CONTRACTOR agrees to provide the services of duly qualified and licensed physicians (each a “Designated Physician”), to perform or do the following:
- i) At the request of COUNTY, to perform and deliver consultative, diagnostic and/or treatment and treatment planning services in the medical specialties described herein, for COUNTY patients through interactive audio, video and/or data communications located in the consult site, maintained by CONTRACTOR as set forth in Section 1.01 (g), and the remote sites, maintained by COUNTY as set forth in Section 1.02, as scheduled;
 - ii) Prepare and submit complete and accurate reports with respect to the services rendered to the COUNTY’s patients, and such other patient information or reports as may be reasonably requested by COUNTY and as may be necessary to create a hospital or clinic health record meeting applicable licensing, accreditation, certification and billing standards;
 - iii) Maintain appropriate medical records documenting the telemedicine encounters in accordance with CONTRACTOR’s standard file maintenance and retention policies otherwise applicable to its own patients. CONTRACTOR shall utilize COUNTY’s InterTrac (or subsequent replacement software) patient record system via direct look up using Virtual Private Network (VPN) access to document psychiatric services rendered by Designated Physician. InterTrac (or subsequent replacement software) notes (e.g. medical service progress notes, psychiatric evaluations, and medication notes) upon completion will be printed, signed by Designated Physician, and the signed originals will be mailed to COUNTY within thirty (30) days following the last day of the month in which the service was provided; and
 - iv) Perform such other and further services as mutually agreed to in writing by both parties.
- (b) Designated Physicians’ Qualifications CONTRACTOR represents to COUNTY that each Designated Physician shall at all times during the term of this Agreement:
- i) be duly qualified and licensed to practice medicine in the State of California;
 - ii) where applicable, hold a current Drug Enforcement Agency narcotic registration certificate;

- iii) maintain all required professional credentials and meet all continuing education requirements necessary to retain board certification or eligibility in the applicable medical specialty;
 - iv) have the qualifications and skills necessary to perform the services required under this Agreement; and
 - v) maintain current status as a Medicare/Medi-Cal provider.
- (c) Method of Performing Services CONTRACTOR or the Designated Physician shall determine the method, details, and means of performing the services described above; provided, however, such services shall be performed in accordance with currently approved and accepted medical standards and procedures, and shall comply with all applicable administrative and clinical rules, procedures and/or regulations concerning the provision of telemedicine services as may be set forth in CONTRACTOR's operating or procedural manuals or as may be otherwise established from time-to-time by CONTRACTOR or required by applicable law, regulation or accreditation or certification standards or COUNTY policy and procedural manuals.
- (d) Time for Performing Services CONTRACTOR shall cause its Designated Physicians to be available to provide services for COUNTY's patients at such times or on such schedules as shall from time-to-time be mutually agreed to in writing by CONTRACTOR and COUNTY. Schedules shall be reviewed monthly by COUNTY and requested changes will be submitted in writing to CONTRACTOR for agreement in advance of scheduling clients.
- (e) Compliance with California and Federal Statutes CONTRACTOR shall cooperate with COUNTY so that COUNTY may meet or satisfy any requirements imposed on it by Title 42, Code of Federal Regulations (CFR), Part 438, and Title 9, California Code of Regulations (CCR), Chapter 11. CONTRACTOR shall cause each Designated Physician to maintain such records and provide such information to COUNTY and to applicable State and Federal regulatory agencies for compliance as may be required by applicable law. Such obligations shall survive the termination of this Agreement. CONTRACTOR agrees to retain such books and records for a term of at least seven (7) years from and after the termination of this Agreement, and further agrees to permit access to and inspection by COUNTY, the California Medical Board, the California Department of Health Services, the United States Department of Health and Human Services, and the Comptroller General of the United States, at all reasonable times and upon demand, of all those facilities, books, and records maintained or utilized by the CONTRACTOR and each Designated Physician in the performance of services pursuant to this Agreement.
- (f) Nondiscrimination CONTRACTOR and each Designated Physician agree:
- i) During the performance of this Agreement, CONTRACTOR and its subcontractors shall not unlawfully discriminate, harass, or allow harassment against any

employee or applicant for employment because of sex, race, color, ancestry, religious creed, national origin, physical disability (including HIV and AIDS), mental disability, medical condition (cancer), age (over 40), marital status, and denial of family care leave. CONTRACTOR and subcontractors shall insure that the evaluation and treatment of their employees and applicants for employment are free from such discrimination and harassment. CONTRACTOR and subcontractors shall comply with the provisions of the Fair Employment and Housing Act (Gov. Code §12990 (a-f) et seq.) and the applicable regulations promulgated thereunder (Title 2 CCR, Section 7285 et seq.). The applicable regulations of the Fair Employment and Housing Commission implementing Government Code Section 12990 (a-f), set forth in Chapter 5 of Division 4 of Title 2 CCR, are incorporated into this Agreement by reference and made a part hereof as if set forth in full. CONTRACTOR and its subcontractors shall give written notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other Agreement.

- ii) Consistent with the requirements of applicable Federal or State law, the CONTRACTOR shall not engage in any unlawful discriminatory practices in the admission of beneficiaries, assignments of accommodations, treatment, evaluation, employment of personnel, or in any other respect on the basis of race, color, gender, religion, marital status, national origin, age, sexual preference or mental or physical handicap.
 - iii) The CONTRACTOR shall comply with the provisions of Section 504 of the Rehabilitation Act of 1973, as amended, pertaining to the prohibition of discrimination against qualified handicapped persons in all federally assisted programs or activities, as detailed in regulations signed by the Secretary of Health and Human Services, effective June 2, 1977, and found in the Federal Register, Volume 42, No. 86, dated May 4, 1977.
 - iv) Notwithstanding other provisions of this section, the CONTRACTOR may require a determination of medical necessity pursuant to Title 9 CCR, Section 1820.205, Section 1830.205 or Section 1830.210, prior to providing covered services to a beneficiary.
 - v) CONTRACTOR shall include the nondiscrimination and compliance provisions of this clause in all subcontracts to perform work under the Agreement.
- (g) Maintenance of CONTRACTOR Facility At all times during the term of this Agreement, CONTRACTOR shall maintain all furniture, equipment, and fixtures located in CONTRACTOR's consult sites in good order, working condition, and repair. CONTRACTOR is responsible for all costs, services, subscriptions, outside services and other fees related to the provisioning and ongoing support of compatible network connectivity for the consult sites.

- (h) Disclosure of Information Except as otherwise required during the performance of services by the Designated Physicians pursuant to this Agreement, neither CONTRACTOR nor any Designated Physician shall, during the term of this Agreement or at any time after the termination of this Agreement, without the written authorization of COUNTY, disclose to any other person or entity, or make use of for their own benefit, any files, records, reports, or other written private or proprietary information concerning the patients, business, methods, operations, financing or services of COUNTY. At the termination of this Agreement, CONTRACTOR shall promptly return to COUNTY all such proprietary information in Physician's possession.
- (i) Patient Information CONTRACTOR and each Designated Physician specifically agree to comply with the requirements of the California Confidentiality of Medical Information Act ("CMIA") and the Federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as referenced in Article V herein. Any failure by CONTRACTOR or a Designated Physician to comply with the applicable CMIA or HIPAA privacy rules shall result, at COUNTY's election, in the immediate termination of this Agreement.
- (j) Remote Access CONTRACTOR and each Designated Physician specifically agree to comply with and sign Exhibit A, marked "Remote Access Request Form," incorporated herein and made by reference a part hereof.

As a user of the COUNTY's information technology resources, CONTRACTOR and each Designated Physician may have access to sensitive resources that are connected through the COUNTY network. To assure security throughout the entire COUNTY network, it is critical that all users actively support and fully comply with the measures described in Exhibit B, marked "El Dorado County Computer and Network Resource Usage Policies and Standards Guide" incorporated herein and made by reference a part hereof. CONTRACTOR also agrees to have Designated Physicians with access to COUNTY computers or software via VPN sign the "County User Agreement," which is contained on page 12 of Exhibit B.

CONTRACTOR shall take all reasonable precautions to ensure that any hardware, software, and/or embedded chip devices used by CONTRACTOR in the performance of services under this Agreement, other than those owned or provided by COUNTY, shall be free from viruses. Nothing in this provision shall be construed to limit any rights or remedies otherwise available to COUNTY under this Agreement.

CONTRACTOR and each Designated Physician specifically agree to act at all times in accordance with all applicable laws and COUNTY policies, rules and procedures, and further agree that they will not use COUNTY information technology resources in an improper or unauthorized manner.

Section 1.02 OBLIGATIONS OF COUNTY

- (a) Remote Sites COUNTY shall provide the required telemedicine equipment, set forth below in its remote sites in Placerville and/or South Lake Tahoe, and shall, during the term of this Agreement, maintain all furniture, equipment, and fixtures located in the remote sites in good order, working condition, and repair.

Equipment to be provided and maintained by COUNTY:

- i) Camera: Tandberg 550 or equivalent.
- ii) Display
- iii) Static IP Address
- iv) High Speed Internet Connection business line with minimum speed up and down of 768kb/s.

COUNTY is responsible for all costs, services, subscriptions, outside services and other fees related to the provisioning and ongoing support of compatible network connectivity for the remote sites. COUNTY represents and warrants to CONTRACTOR that at all times during the term of this Agreement, the remote sites will be facilities that are otherwise eligible to be originating sites for the receipt of telemedicine services under applicable State and/or Federal laws, including but not limited to, the rules and regulations promulgated by the Center for Medicare and Medicaid Services ("CMS").

- (b) Telemedicine Coordinator (TM Coordinator) At all times during the term of this Agreement, COUNTY shall provide and designate one (1) or more of its employees or staff who will be responsible for scheduling, obtaining and communicating necessary information to CONTRACTOR and its Designated Physicians, coordinating the presentation of COUNTY's patients, and other duties to ensure the successful presentation of the patient to CONTRACTOR's Designated Physician in connection with the rendering of services.
- (c) COUNTY's Patients With respect to each of COUNTY's patients for whom services are to be provided by CONTRACTOR's Designated Physicians pursuant to this Agreement, COUNTY agrees to obtain, or provide, at its cost and expense, the following:
- i) COUNTY shall obtain Exhibit C, marked "Patient Consent Form," incorporated herein and made by reference a part hereof, from the patient or the patient's legal representative prior to the delivery of the services by CONTRACTOR's Designated Physician.

- ii) Prior to CONTRACTOR's delivery of services, COUNTY's TM Coordinator shall provide CONTRACTOR with all information concerning COUNTY's patient which is necessary and appropriate for the provision of services, including, but not limited to:
 - 1. the services that are requested to be performed with respect to the patient;
 - 2. the patient's eligibility to receive the requested services; and
 - 3. the patient's medical history, vitals (as needed), labs, and test results related to the condition being presented and for which the services are to be performed.

The foregoing information shall be available to CONTRACTOR via direct look up using VPN access to the InterTrac (or subsequent replacement software) medical records system.

- iii) At the time that the services are delivered to COUNTY's patient at a remote site, the patient shall be presented by COUNTY's staff, medical personnel and/or the patient's primary care physician who is otherwise qualified to interact with the Designated Physician in connection with the delivery of services pursuant to protocols, processes and procedures as agreed upon by COUNTY Medical Administrative Officer, or designee, and CONTRACTOR.
 - iv) Prior to providing services, CONTRACTOR shall review the patient's consent to telemedicine services and determine whether it is adequate. CONTRACTOR shall not perform telemedicine services without an adequate informed consent.
- (d) Patient Records and Files COUNTY shall keep, maintain, and store all business records and patient files relating to COUNTY's patients for whom services are rendered by CONTRACTOR pursuant to this Agreement. All original patient records shall remain the property of COUNTY; provided, however, CONTRACTOR shall have the right, both during and following the termination of this Agreement, to inspect and copy any such records or files relating to the services performed by the Designated Physicians for any reasonable or necessary medical, business, governmental or other legal purpose permitted by applicable law and regulation.
- (e) Cooperation of COUNTY COUNTY agrees to comply with all reasonable requests of CONTRACTOR or the Designated Physicians, and shall provide CONTRACTOR or the Designated Physicians with or access to all documents or information reasonably necessary to the performance of the Designated Physician's services pursuant to this Agreement.

Article II. TERM

This Agreement shall become effective upon final signature and shall expire June 30, 2011 unless earlier terminated pursuant to the provisions under Article XII or Article XIII herein.

Article III. COMPENSATION FOR SERVICES

Section 3.01 CONTRACTOR shall submit monthly invoices no later than thirty (30) days following the end of a "service month" except in those instances where CONTRACTOR obtains written approval from County Health Services Department (HSD) Director or Director's designee granting an extension of the time to complete billing for services or expenses. For billing purposes, a "service month" shall be defined as a calendar month during which CONTRACTOR provides services in accordance with ARTICLE I, "Scope of Services."

Section 3.02 For services provided herein, COUNTY agrees to pay CONTRACTOR monthly in arrears and within forty-five (45) days following the COUNTY's receipt and approval of itemized invoice(s) identifying services rendered. Each monthly invoice shall describe:

- a. Client name
- b. Dates of service
- c. Service type
- d. Duration of service

Section 3.03 CONTRACTOR shall not charge any clients or third party payors any fee for service.

Section 3.04 It is expressly understood and agreed between the parties hereto that the COUNTY shall make no payment for COUNTY-responsible clients and have no obligation to make payment to CONTRACTOR unless the services provided by CONTRACTOR hereunder received prior written authorization from HSD Director or the Director's designee. It is further agreed that COUNTY shall make no payments for services unless CONTRACTOR has provided COUNTY with evidence of insurance coverage as outlined in ARTICLE XVI hereof. COUNTY may provide retroactive authorization when special circumstances exist, as determined by the HSD Director or the Director's designee, based upon CONTRACTOR's written request.

Section 3.05 In accordance with Title 9 CCR, Section 565.5, reimbursement for services under this Agreement shall be limited to persons who are unable to obtain private care. Such persons are those who are unable to pay for private care or for whom no private care is available within a reasonable distance from their residence.

Section 3.06 It is understood that any payments received from COUNTY for services rendered under this Agreement shall be considered as payment in full and CONTRACTOR cannot look to any other source for reimbursement for the services provided under this Agreement, except with specific authorization from the HSD Director.

Section 3.07 Rates: COUNTY will compensate CONTRACTOR at the following hourly rates:

<u>Medical Specialty</u>	<u>Hourly Rate</u>
Psychiatry	\$250
Other medical specialties as requested (Such as Infectious Disease Consulting)	\$300

Section 3.08 Designated Physicians may be scheduled to provide services for a minimum of one (1) hour. The length of a scheduled client appointment may be less than or more than an hour.

Section 3.09 With the exceptions noted in the paragraphs below, COUNTY is required to compensate CONTRACTOR for the scheduled patient time for each scheduled appointment for service, even if the actual telemedicine session ends sooner than the scheduled time. If the actual telemedicine session takes longer than scheduled, COUNTY will compensate CONTRACTOR for the extended time in quarter hour increments. Example:

- If Designated Physician's scheduled time is for two and one-half (2.5) hours, COUNTY will compensate CONTRACTOR for two and one-half (2.5) hours, even if the scheduled session actually takes only two (2) hours.
- If the telemedicine session takes two (2) hours and thirty-five (35) minutes, COUNTY will compensate CONTRACTOR for two (2) hours and forty-five (45) minutes (i.e. an extra quarter hour increment).

Section 3.10 Costs for the completion and submission of the associated and required clinical documentation for the medical record noted in Article I, Section 1.01 (a) ii and iii are covered within the rate for the scheduled patient time.

Section 3.11 If a scheduled session is cancelled or reduced by COUNTY less than forty-eight (48) hours prior to the session start time, COUNTY will compensate CONTRACTOR for the complete scheduled time for the session based upon the compensation described above.

Section 3.12 If a scheduled session is cancelled by Designated Physician, or is cancelled by COUNTY with forty-eight (48) hours or more notice by COUNTY, no payment will be due from COUNTY. If the time for a scheduled session is reduced by COUNTY with forty-eight (48) or more hours notice, COUNTY's obligation for payment will be based upon the reduced scheduled appointment time.

Section 3.13 Not-to-Exceed: \$58,500 over the term of this Agreement.

Section 3.14 Invoices shall be submitted to:

Health Services Department – Mental Health Division
929 Spring Street
Placerville, CA 95667
Attn: Accounts Payable

Article IV. TERMS AND CONDITIONS

CONTRACTOR shall meet all terms and conditions specified in the County's agreement with California Department of Mental Health, as stated in Exhibits D, D-1 and D-2, marked "State Required Terms and Conditions," incorporated herein and made by reference a part hereof.

Article V. HIPAA COMPLIANCE

As a condition of CONTRACTOR performing services for the County of El Dorado, CONTRACTOR shall comply with Exhibit E, marked "HIPAA Business Associate Agreement," incorporated herein and made by reference a part hereof.

Article VI. MANDATED REPORTER REQUIREMENTS

CONTRACTOR acknowledges and agrees to comply with mandated reporter requirements pursuant to the provisions of Article 2.5 (commencing with Section 11164) of Chapter 2 of Title 1 of Part 4 of the California Penal Code, also known as The Child Abuse and Neglect Reporting Act.

Article VII. DEBARMENT AND SUSPENSION CERTIFICATION

By signing this agreement, the CONTRACTOR agrees to comply with applicable Federal suspension and debarment regulations including, but not limited to 45 CFR 76.

By signing this agreement, the CONTRACTOR certifies to the best of its knowledge and belief, that it and its principals:

- (a) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal department or agency;
- (b) Have not within a three year period preceding this application/proposal/agreement been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification of destruction of records, making false statements, or receiving stolen property;

- (c) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with commission of any of the offenses enumerated in Paragraph b(2) herein;
- (d) Have not within a three (3) year period preceding this application/proposal/agreement had one or more public transactions (Federal, State or local) terminated for cause or default;
- (e) Shall not knowingly enter in to any lower tier covered transaction with a person who is proposed for debarment under Federal regulations (i.e., 48 CFR part 9, subpart 9.4), debarred, suspended, declared ineligible or voluntarily excluded from participation in such transactions, unless authorized by the State; and
- (f) Shall include a clause entitled, "Debarment and Suspension Certification" that essentially sets forth the provisions herein, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

If the CONTRACTOR is unable to certify to any of the statements in this certification, the CONTRACTOR shall submit an explanation to COUNTY.

The terms and definitions herein have the meanings set out in the Definitions and Coverage sections of the rules implementing Federal Executive Order 12549.

If the CONTRACTOR knowingly violates this certification, in addition to other remedies available to the Federal Government, COUNTY may terminate this agreement for cause or default.

Article VIII. CHANGES TO AGREEMENT

This Agreement may be amended by mutual consent of the parties hereto. Said amendments shall become effective only when in writing and fully executed by duly authorized officers of the parties hereto.

Article IX. CONTRACTOR TO COUNTY

It is understood that the services provided under this Agreement shall be prepared in and with cooperation from COUNTY and its staff. It is further agreed that in all matters pertaining to this Agreement, CONTRACTOR shall act as Contractor only to COUNTY and shall not act as Contractor to any other individual or entity affected by this Agreement nor provide information in any manner to any party outside of this Agreement that would conflict with CONTRACTOR's responsibilities to COUNTY during term hereof.

Article X. ASSIGNMENT AND DELEGATION

CONTRACTOR is engaged by COUNTY for its unique qualifications and skills as well as those of its personnel. CONTRACTOR shall not subcontract, delegate or assign services to be provided, in whole or in part, to any other person or entity without prior written consent of COUNTY.

Article XI. INDEPENDENT CONTRACTOR/LIABILITY

CONTRACTOR is, and shall be at all times, deemed independent and shall be wholly responsible for the manner in which it performs services required by terms of this Agreement. CONTRACTOR exclusively assumes responsibility for acts of its employees, associates, and subcontractors, if any are authorized herein, as they relate to services to be provided under this Agreement during the course and scope of their employment.

CONTRACTOR shall be responsible for performing the work under this Agreement in a safe, professional, skillful and workmanlike manner and shall be liable for its own negligence and negligent acts of its employees. COUNTY shall have no right of control over the manner in which work is to be done and shall, therefore, not be charged with responsibility of preventing risk to CONTRACTOR or its employees.

Article XII. FISCAL CONSIDERATIONS

Section 12.01 The parties to this Agreement recognize and acknowledge that COUNTY is a political subdivision of the State of California. As such, the County of El Dorado is subject to the provisions of Article XVI, Section 18 of the California Constitution and other similar fiscal and procurement laws and regulations and may not expend funds for products, equipment or services not budgeted in a given fiscal year. It is further understood that in the normal course of COUNTY business, COUNTY will adopt a proposed budget prior to a given fiscal year, but that the final adoption of a budget does not occur until after the beginning of the fiscal year.

Section 12.02 Notwithstanding any other provision of this Agreement to the contrary, COUNTY shall give notice of cancellation of this Agreement in the event of adoption of a proposed budget that does not provide for funds for the services, products or equipment subject herein. Such notice shall become effective upon the adoption of a final budget which does not provide funding for this Agreement. Upon the effective date of such notice, this Agreement shall be automatically terminated and COUNTY released from any further liability hereunder.

Section 12.03 In addition to the above, should the Board of Supervisors during the course of a given year for financial reasons reduce, or order a reduction, in the budget for any COUNTY department for which services were contracted to be performed, pursuant to this paragraph in the sole discretion of the COUNTY, this Agreement may be deemed to be canceled in its entirety subject to payment for services performed prior to cancellation.

Article XIII. DEFAULT, TERMINATION, AND CANCELLATION

Section 13.01 Default

Upon the occurrence of any default of the provisions of this Agreement, a party shall give written notice of said default to the party in default (notice). If the party in default does not cure the default within ten (10) days of the date of notice (time to cure), then such party shall be in default. The time to cure may be extended at the discretion of the party giving notice. Any extension of time to cure must be in writing, prepared by the party in default for signature by the

party giving notice and must specify the reason(s) for the extension and the date on which the extension of time to cure expires.

Notice given under this section shall specify the alleged default and the applicable Agreement provision and shall demand that the party in default perform the provisions of this Agreement within the applicable period of time. No such notice shall be deemed a termination of this Agreement unless the party giving notice so elects in this notice, or the party giving notice so elects in a subsequent written notice after the time to cure has expired. In the event of termination for default, COUNTY reserves the right to take over and complete the work by contract or by any other means.

Section 13.02 Bankruptcy

This Agreement, at the option of the COUNTY, shall be terminable in the case of bankruptcy, voluntary or involuntary, or insolvency of CONTRACTOR.

Section 13.03 Ceasing Performance

COUNTY may terminate this Agreement in the event CONTRACTOR ceases to operate as a business, or otherwise becomes unable to substantially perform any term or condition of this Agreement.

Section 13.04 Termination or Cancellation without Cause

COUNTY may terminate this Agreement in whole or in part upon seven (7) calendar days written notice by COUNTY without cause. If such prior termination is effected, COUNTY will pay for satisfactory services rendered prior to the effective dates as set forth in the Notice of Termination provided to CONTRACTOR, and for such other services, which COUNTY may agree to in writing as necessary for contract resolution. In no event, however, shall COUNTY be obligated to pay more than the total amount of the contract. Upon receipt of a Notice of Termination, CONTRACTOR shall promptly discontinue all services affected, as of the effective date of termination set forth in such Notice of Termination, unless the notice directs otherwise.

Article XIV. NOTICE TO PARTIES

All notices to be given by the parties hereto shall be in writing and served by depositing same in the United States Post Office, postage prepaid and return receipt requested.

Notices to COUNTY shall be addressed as follows:

COUNTY OF EL DORADO
HEALTH SERVICES DEPARTMENT
931 SPRING STREET
PLACERVILLE, CA 95667
ATTN: NEDA WEST, DIRECTOR

or to such other location as the COUNTY directs.

Notices to CONTRACTOR shall be addressed as follows:

CLINICIANS TELEMED MEDICAL GROUP, INC.
1801 16TH STREET, SUITE B
BAKERSFIELD, CA 93301
ATTN: JOHNSON JUNG, PRESIDENT

or to such other location as the CONTRACTOR directs.

Article XV. INDEMNITY

The CONTRACTOR shall defend, indemnify, and hold the COUNTY harmless against and from any and all claims, suits, losses, damages and liability for damages of every name, kind and description, including attorneys fees and costs incurred, brought for, or on account of, injuries to or death of any person, including but not limited to workers, COUNTY employees, and the public, or damage to property, or any economic or consequential losses, which are claimed to or in any way arise out of or are connected with the CONTRACTOR's services, operations, or performance hereunder, regardless of the existence or degree of fault or negligence on the part of the COUNTY, the CONTRACTOR, subcontractor(s) and employee(s) of any of these, except for the sole, or active negligence of the COUNTY, its officers and employees, or as expressly prescribed by statute. This duty of CONTRACTOR to indemnify and save COUNTY harmless includes the duties to defend set forth in California Civil Code Section 2778.

Article XVI. INSURANCE

Section 16.01 CONTRACTOR shall provide proof of a policy of insurance satisfactory to the County of El Dorado Risk Manager and documentation evidencing that CONTRACTOR maintains insurance that meets the following requirements:

- a) Full Workers' Compensation and Employers' Liability Insurance covering all employees of CONTRACTOR as required by law in the State of California.
- b) Commercial General Liability Insurance of not less than \$1,000,000 combined single limit per occurrence for bodily injury and property damage.
- c) Automobile Liability Insurance of not less than \$1,000,000 is required in the event motor vehicles are used by the CONTRACTOR in the performance of the Agreement.

Section 16.02 In the event CONTRACTOR is a licensed professional, and is performing professional services under this Agreement, professional liability (for example, malpractice insurance) is required with a limit of liability of not less than \$1,000,000 per occurrence.

Section 16.03 CONTRACTOR shall furnish a certificate of insurance satisfactory to the County of El Dorado Risk Manager as evidence that the insurance required above is being maintained.

Section 16.04 The insurance will be issued by an insurance company acceptable to Risk Management, or be provided through partial or total self-insurance likewise acceptable to Risk Management.

Section 16.05 CONTRACTOR agrees that the insurance required above shall be in effect at all times during the term of this Agreement. In the event said insurance coverage expires at any time or times during the term of this Agreement, CONTRACTOR agrees to provide at least thirty (30) days prior to said expiration date, a new certificate of insurance evidencing insurance coverage as provided for herein for not less than the remainder of the term of the Agreement, or for a period of not less than one (1) year. New certificates of insurance are subject to the approval of Risk Management and CONTRACTOR agrees that no work or services shall be performed prior to the giving of such approval. In the event the CONTRACTOR fails to keep in effect at all times insurance coverage as herein provided, COUNTY may, in addition to any other remedies it may have, terminate this Agreement upon the occurrence of such event.

The certificate of insurance must include the following provisions stating that:

- (a) The insurer will not cancel the insured's coverage without thirty (30) days prior written notice to COUNTY, and;
- (b) The County of El Dorado, its officers, officials, employees, and volunteers are included as additional insured, but only insofar as the operations under this Agreement are concerned. This provision shall apply to the general liability policy.

Section 16.06 The CONTRACTOR's insurance coverage shall be primary insurance as respects the COUNTY, its officers, officials, employees and volunteers. Any insurance or self-insurance maintained by the COUNTY, its officers, officials, employees or volunteers shall be excess of the CONTRACTOR's insurance and shall not contribute with it.

Section 16.07 Any deductibles or self-insured retentions must be declared to and approved by the COUNTY, either: the insurer shall reduce or eliminate such deductibles or self-insured retentions as respects the COUNTY, its officers, officials, employees, and volunteers; or the CONTRACTOR shall procure a bond guaranteeing payment of losses and related investigations, claim administration and defense expenses.

Section 16.08 Any failure to comply with the reporting provisions of the policies shall not affect coverage provided to the COUNTY, its officers, officials, employees or volunteers.

Section 16.09 The insurance companies shall have no recourse against the County of El Dorado, its officers and employees or any of them for payment of any premiums or assessments under any policy issued by any insurance company.

Section 16.10 CONTRACTOR's obligations shall not be limited by the foregoing insurance requirements and shall survive expiration of this Agreement.

Section 16.11 In the event CONTRACTOR cannot provide an occurrence policy, CONTRACTOR shall provide insurance covering claims made as a result of performance of this Agreement for not less than three (3) years following completion of performance of this Agreement.

Section 16.12 Certificate of insurance shall meet such additional standards as may be determined by the contracting County Department either independently or in consultation with Risk Management, as essential for the protection of the COUNTY.

Article XVII. INTEREST OF PUBLIC OFFICIAL

No official or employee of COUNTY who exercises any functions or responsibilities in review or approval of services to be provided by CONTRACTOR under this Agreement shall participate in or attempt to influence any decision relating to this Agreement which affects personal interest or interest of any corporation, partnership, or association in which he/she is directly or indirectly interested; nor shall any such official or employee of COUNTY have any interest, direct or indirect, in this Agreement or the proceeds thereof.

Article XVIII. INTEREST OF CONTRACTOR

CONTRACTOR covenants that CONTRACTOR presently has no personal interest or financial interest, and shall not acquire same in any manner or degree in either: 1) any other contract connected with or directly affected by the services to be performed by this Agreement; or, 2) any other entities connected with or directly affected by the services to be performed by this Agreement. CONTRACTOR further covenants that in the performance of this Agreement no person having any such interest shall be employed by CONTRACTOR.

Article XIX. CONFLICT OF INTEREST

The parties to this Agreement have read and are aware of the provisions of Government Code Section 1090 et seq. and Section 87100 relating to conflict of interest of public officers and employees. CONTRACTOR attests that it has no current business or financial relationship with any COUNTY employee(s) that would constitute a conflict of interest with provision of services under this contract and will not enter into any such business or financial relationship with any such employee(s) during the term of this Agreement. COUNTY represents that it is unaware of any financial or economic interest of any public officer or employee of CONTRACTOR relating to this Agreement. It is further understood and agreed that if such a financial interest does exist at the inception of this Agreement either party may immediately terminate this Agreement by giving written notice as detailed in the Article in the Agreement titled, "Default, Termination and Cancellation."

Article XX. CALIFORNIA RESIDENCY (FORM 590)

All independent Contractors providing services to the COUNTY must file a State of California Form 590, certifying their California residency or, in the case of a corporation, certifying that they have a permanent place of business in California. The Contractor will be required to

submit a Form 590 prior to execution of an Agreement or COUNTY shall withhold seven (7) percent of each payment made to the CONTRACTOR during term of the Agreement. This requirement applies to any agreement/contract exceeding \$1,500.

Article XXI. TAXPAYER IDENTIFICATION NUMBER (FORM W-9)

All independent Contractors or corporations providing services to the COUNTY must file a Department of the Treasury Internal Revenue Service Form W-9, certifying their Taxpayer Identification Number.

Article XXII. COUNTY BUSINESS LICENSE

It is unlawful for any person to furnish supplies or services, or transact any kind of business in the unincorporated territory of the County of El Dorado without possessing a County business license unless exempt under County Code Section 5.08.070.

Article XXIII. ADMINISTRATOR

The COUNTY Officer or employee with responsibility for administering this Agreement is Christine Kondo-Lister, Deputy Director, Health Services Department, Mental Health Division, or successor.

Article XXIV. AUTHORIZED SIGNATURES

The parties to this Agreement represent that the undersigned individuals executing this Agreement on their respective behalf are fully authorized to do so by law or other appropriate instrument and to bind upon said parties to the obligations set forth herein.

Article XXV. PARTIAL INVALIDITY

If any provision of this Agreement is held by a court of competent jurisdiction to be invalid, void or unenforceable, the remaining provisions will continue in full force and effect without being impaired or invalidated in any way.

Article XXVI. VENUE

Any dispute resolution action arising out of this Agreement, including, but not limited to, litigation, mediation, or arbitration, shall be brought in the County of El Dorado, California, and shall be resolved in accordance with the laws of the State of California.

Article XXVII. ENTIRE AGREEMENT

This document and the documents referred to herein or exhibits hereto are the entire Agreement between the parties and they incorporate or supersede all prior written or oral Agreements or understandings.

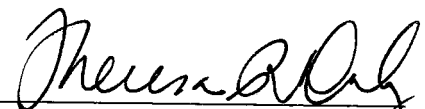
REQUESTING DEPARTMENT HEAD CONCURRENCE:

By 
Neda West, Director
Health Services Department

Dated: 1-17-11

IN WITNESS WHEREOF, the parties hereto have executed this Agreement on the dates indicated below.

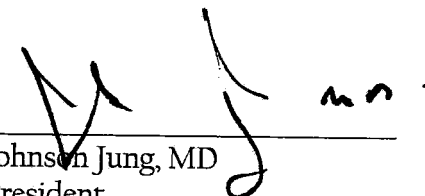
--COUNTY OF EL DORADO--

By: 
Theresa R. Daly, Purchasing Agent
Chief Administrative Office
"COUNTY"

Dated: 1/25/11

-- CONTRACTOR --

CLINICIANS TELEMED MEDICAL GROUP, INC.
A CALIFORNIA CORPORATION

By: 
Johnson Jung, MD
President
"CONTRACTOR"

Dated: 1/20/11

By: 
Corporate Secretary

Dated: 1/20/11



EXHIBIT A REMOTE ACCESS REQUEST FORM



Access may be granted to a single individual using a single computer only. User Ids cannot be shared and passwords must not be revealed. Access is for legitimate El Dorado County business use only and may be revoked at any time.

1. Person requesting access:

Name: _____
Employer/Dept.: _____
Address: _____
Phone #: _____ Email: _____

2. Who owns the computer that will be used to access El Dorado County resources?

El Dorado County Public Agency Private Company Personal

3. Whom shall we contact in the future if we shut down access?

4. What services will you use when connected to EDC network?

County E-Mail Mainframe (FAMIS, LMIS, M204, etc.) EDCNET
 Mapped Drives Application Server FTP
 Other (please specify): _____

5. What applications/files are you using/supporting for El Dorado County?

6. Do you need remote access to County resources outside of business hours, Monday – Friday, 7 a.m. – 6 p.m.? YES NO If YES, please state times and reasons:

7. What Antivirus Program is installed on the computer? None

McAfee AV Symantec AV Other: _____

8. What virus signature file version is being used currently? _____

9. Are daily checks performed for operating system and antivirus updates, and are they installed as soon as updates are available? YES NO

10. Does this computer need to dial up with a modem to get to the Internet?

YES NO

11. Does this computer connect to a local network? YES NO

If YES, please list device types connected to the network (computers, printers, hub, etc):

12. Do you use a firewall on your network? YES NO

If YES, what brand? _____

13. Do you have a software firewall installed on your computer? YES NO

If YES what kind?

Norton Firewall McAfee Firewall Black Ice Firewall

Other: _____

14. Do you use remote control / remote access software to support County applications?

YES NO

If YES what kind?

PC Anywhere Telnet Terminal Services

Other: _____ Port used: _____

If you have questions or need assistance, please call IT Help Desk at (530)621-5696

I have read and understand that:

- 1) As a user of the County's information technology resources, I may have access to sensitive resources that are connected through the County network. To assure security throughout the entire County network, it is critical that all users actively support and fully comply with the measures described in the Computer and Network Resource Usage Policies and Standards Guide. Failure to comply can place the entire County network at serious risk. Failure to comply may subject me to disciplinary action.
- 2) As a User of the County's information systems I shall at all times act in accordance with all applicable laws and County policies, rules or procedures. I shall not use County information technology resources in an improper or unauthorized manner.

I have read, understand and am fully aware of the El Dorado County Computer and Network Resource Usage Policies and Standards Guide. I agree to comply with the terms of this policy.

**Applicant
Print Name:**

Signature: _____

Date: _____

**Department
Head Name:**

Signature: _____

Date: _____

TO BE COMPLETED BY INFORMATION TECHNOLOGIES PERSONNEL

- | | |
|------------------------------|----------------------------------|
| <input type="checkbox"/> RAS | <input type="checkbox"/> VPN |
| <input type="checkbox"/> FTP | <input type="checkbox"/> TN 3270 |

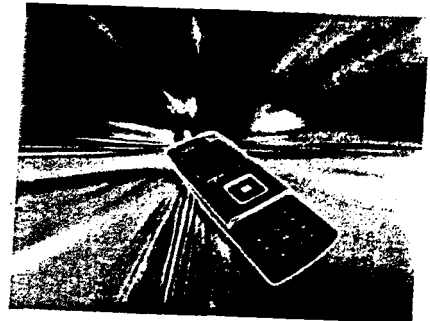
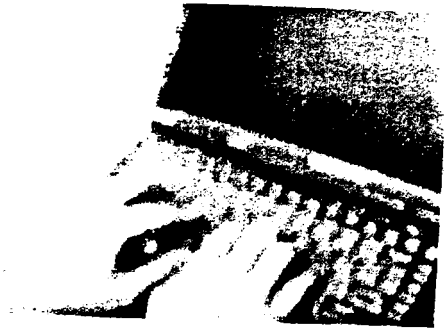
Security Officer Authorization:	
GWI ticket #:	
Account Information Verified By:	
Account created by:	
Date:	
Time	
Please List Time Allowed Outside Normal Mon.-Fri. 7 a.m. – 6 p.m.:	
User ID:	

Comments:

El Dorado County

Computer and Network Resource Usage Policies and Standards Guide

General Use



Approved by the Board of Supervisors August 18, 2009

INTRODUCTION

This Computer and Network Resource Usage Policies and Standards Guide has been created to assist El Dorado County employees in understanding their responsibilities when using County computer workstations, printers, peripherals, software, and network resources. The Guide is intended to comply with Board Policy A-19 and applies to all County employees.

There are a number of changes to this latest revision of the Computer and Network Usage Policies and Standards Guide. The majority of these changes are driven by new regulations from various government agencies that necessitate an increased focus on security and the protection against loss or theft of data in protected classes. These classes include the Health Insurance Portability and Accountability Act (HIPAA), Personally Identifiable Information (PII) and Protected Health Information (PHI), Sarbanes-Oxley, etc.)

Page 12, "El Dorado County Computer and Network Resource Usage Policies Agreement" must be signed by all County employees indicating they have read and understood the General Usage Policies, "1.1 – Background" through "1.14 – Remote Access Policies".

It is mandatory that the employee sign the Agreement on an annual basis. It is suggested that the employee re-sign the Agreement at the time of their annual evaluation.

SECTION 1 TABLE OF CONTENTS

1	GENERAL USAGE POLICIES.....	1
	1.1 Background	1
	1.2 Purpose.....	1
	1.3 General Use and Ownership	2
	1.4 Use of Personally Owned Software and Equipment	3
	1.5 Compliance with Software Copyright Laws	3
	1.6 Disposal of Copyrighted Software Material	3
	1.7 Use of Computer Resources.....	3
	1.8 Use of Electronic Communication	4
	1.8.1 Definitions	4
	1.8.2 Personal Use.....	5
	1.8.3 State and Federal Laws	5
	1.8.4 Restrictions	6
	1.8.5 False Identity.....	6
	1.8.6 Representation.....	6
	1.8.7 Network Capacity.....	6
	1.8.8 Possession.....	6
	1.9 Use of the Internet.....	7
	1.10 Computer User ID's and Password	7
	1.11 Computer Viruses	8
	1.12 Removable Data Storage Devices	8
	1.13 Portable Computing Devices (WPDA, PDA, Laptops, Tablets)	9
	1.14 Remote Access	10
2	COUNTY USER AGREEMENT.....	12
3	GENERAL USAGE STANDARDS AND GUIDELINES	13
	3.1 Electronic Communication	13
	3.1.1 Security and Confidentiality	13
	3.1.2 Anti-Spam Measures	13
	3.1.3 HIPPA and Compliance with Electronic Communication Privacy Act.....	14
	3.1.4 E-mail Retention.....	14

3.1.5	Managing E-mail	14
3.1.6	Electronic Communications – Instant Messaging	16
3.2	Passwords	16
3.2.1	Password Construction Guidelines	16
3.2.2	Password Protection Standards.....	17
3.2.3	Application Development Password Standards.....	18
3.2.4	Pass Phrases	18
3.2.5	Use of Passwords and Pass Phrases for Remote Access Users.....	19
3.3	Server Storage Utilization	19
3.3.1	File Storage Options	19
3.3.2	Server File Storage	19

GENERAL USAGE POLICIES

1.1 Background

El Dorado County has an extensive communication infrastructure with network and computing resources for use by County employees, contractors, vendors, quasi-governmental employees (fire departments, community services districts, etc.) and temporary workers, hereafter referred to as "County User". In addition, the County provides a large and continuously growing number of computer workstations, printers, peripherals, software, training, and supplies to all County sites. These items are provided by El Dorado County to allow County Users to perform tasks efficiently to meet the goals established by the El Dorado County Board of Supervisors.

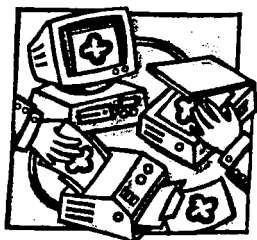


While most are familiar with the term "computer", it is only one of the resources that are collectively known as network resources. Network resources consist of computers and their associated peripherals. These network resources, applications, and data provide the means to deliver services to El Dorado County residents.

While much of the data used by El Dorado County is "public" information, with legislative changes (HIPAA, PII, PHI, Sarbanes-Oxley, etc.) there is a need to safeguard the data the County uses and to maintain the security and privacy of that data. Automatic and procedural security controls are in place to prevent or reduce unauthorized access to these resources. The primary responsibility for maintaining the integrity, security, and privacy of this information and its resources lies with the County User.

All computer systems furnished by the County, including but not limited to computer equipment, software, operating systems, storage media, and network accounts providing electronic communication, file storage, Internet access ("www" browsing, use groups, etc.) and FTP (File Transfer Protocol), are the property of El Dorado County. These systems are to be used for business purposes in serving the interests of the County in the course of normal operations. Improper use of any of these resources can result in lost or degraded services to some or all County Users. Violation of local, State and Federal laws, rules and policies may call for prosecution under the law, including fines and imprisonment and disciplinary action.

County Users are responsible for reading, understanding, and following the appropriate use of County equipment and the release of County data. This document summarizes policies and offers standards and guidelines regarding the integrity, security, and privacy of County data, network resources and computers. County Users should contact their supervisors for any necessary clarification.



1.2 Purpose

The purpose of these policies is to define the acceptable use of computer equipment and networked resources throughout El Dorado County. These policies are in place to protect the County User and El Dorado County. Inappropriate use exposes El Dorado County to risks including but not limited to virus attacks, compromising network systems and services, and potential civil or criminal litigation. These

policies apply to all computer equipment that is used by County Users or any device connected to the El Dorado County network.

Deviations from these policies may occur based on specific departmental technical needs. Deviations must be reviewed and approved by the Director, Information Technologies (I.T.) or designee. I.T. decisions may be appealed to the IT Steering Committee.

1.3 General Use and Ownership

The County's business information, telephone, network, computer and software resources, peripherals and supplies are County property and are intended to be used to conduct County business. They do not belong to individuals and are used by County Users for the purpose of completing the work required for their position while employed or contracted by the County.



All data created or received on the County's computer systems remains the property of El Dorado County. There is no reasonable expectation of privacy regarding the confidentiality of information stored on any computer, terminal or network device belonging to El Dorado County, whether related to County business or to personal use.

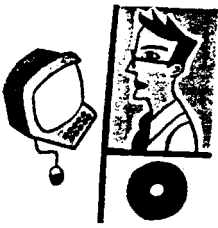
It is the responsibility of the County User to safeguard confidential information from unauthorized disclosure or use. County Users shall not seek to use personal or confidential information for their own use or personal gain. County Users must take all reasonable precautions to ensure privacy is maintained under the law while handling information in any form, including but not limited to voice, electronic (disk file, diskette, CD ROM, DVD, magnetic tape, electronic communication, etc.), paper, photograph, and microfiche information.

New regulatory requirements dictate computers processing protected classes of information (HIPAA, PII, PHI Sarbanes-Oxley, etc.) have their hard drives encrypted. Additionally portable media devices used to store protected classes of information must also be encrypted (USB storage devices, etc.). Portable computers (laptops, notebooks, cellular based personal digital assistants (CPDA)) must be encrypted, contain software designed to recover lost or stolen devices, and have the ability to be remotely incapacitated and able to destroy all data on the device).

Access to another County User's data will not be granted without written or electronic communication authorization from the appropriate department head or designee. All electronically stored data remains the property of El Dorado County; intentional destruction of this property is prohibited.

County Users are responsible for exercising good judgment regarding the reasonableness of personal use on personal time. County Users may engage in reasonable incidental personal use of the County's computer systems, to the extent permitted by the County User's department head, as long as such use does not degrade overall system performance (such as streaming media, i.e. music or video files), detract from a County User's productivity, duties, service to the public or to the County, violate any law, or any County policy, procedure, or regulation or tarnish the image of the County or contribute to the disrepute of the County.

For security and network maintenance purposes, I.T. staff members may monitor equipment, systems and network traffic at any time. This monitoring shall be done under the auspices of this policy, which is incorporated into Board Policy A-19.

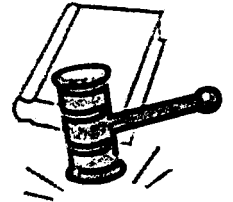


1.4 Use of Personally Owned Software and Equipment

Personally owned software may not be installed on County computers, nor shall personally owned computer hardware or peripheral equipment be connected to County computers or attached to the County network.

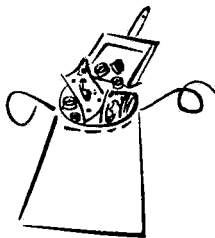
1.5 Compliance with Software Copyright Laws

A copyright violation exposes the County to substantial risk of legal liability. County Users may not:



- Install any software without having proof of licensing; or
- Install software licensed for one workstation on multiple machines; or
- Install or distribute "pirated" or other software products that are not appropriately licensed for use by El Dorado County; or
- Install personal or non-County standard software or peripherals.

County Users may not make unauthorized copies of copyrighted material including, but not limited to, photographs from magazines, books or other copyrighted sources, copyrighted music, or any copyrighted software for which the County or the County User does not have a valid license.

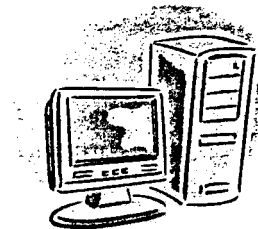


1.6 Disposal of Copyrighted Software Material

All copyrighted material must be disposed of in such a way as to render it useless and to minimize the potential liability to the County. The media on which the copyrighted material was obtained must be physically destroyed (for example, CDs, DVDs or floppy disks, will be broken in half or shredded) and any license keys or any other information that is required in order to use the software legally must be destroyed.

1.7 Use of Computer Resources

County computer resources are used by hundreds of County Users. To ensure that these resources are available and working properly, personal use of these resources must not negatively impact others.



No County User may attempt to access computer systems, or their resources, unless proper authorization has been granted by the department head. Any attempt to maliciously alter, erase, damage, destroy or make otherwise unusable any data, software, computer, or network system may constitute a felony and may result in any combination of

disciplinary action and/or prosecution and fines, including litigation costs and payment of damages under applicable Local, State, and Federal statutes.

No County User shall willfully or through negligence introduce a malicious program into the network, any server or computer, (e.g. virus, worm, Trojan horse, electronic communication bomb etc.), nor shall any County User use port scanners or other intrusive software intended to undermine the stability and integrity of the County network and attached resources.

No County User shall use a County computing resource to engage in procuring, viewing or transmitting material that is pornographic in nature or is in violation of sexual harassment or hostile workplace guidelines. In general, any material that may be considered objectionable or may tend to bring the County into disrepute may not be sent via the County's computer systems.

El Dorado County has a significant investment in network server hardware and associated data storage capacity. Please see General Usage Standards and Guidelines – 3.3 Server Storage Utilization for options and recommendations for the file storage options, directory structure and back-ups to maximize available server storage space.



1.8 Use of Electronic Communication

The need to manage electronic communication systems properly can be viewed the same as other records keeping systems; namely, to ensure compliance with laws concerning the creation, retention, or access to such electronic communication documents and to manage resources storing such electronic communication documents.

El Dorado County government agencies that use electronic communications have an obligation to make County Users aware that electronic communication messages, like paper records, must be retained and destroyed according to established records management procedures. They should deploy, or modify, electronic communication systems to facilitate electronic records management. Specific procedures and processes will vary according to departmental needs and the particular requirements placed on them via specific governmental agency rules or applicable law.

Please see General Usage Standards and Guidelines – 3.1 Electronic Communication for detail standards in support of these policies.

1.8.1 Definitions

Electronic communication **systems** transport messages (store and deliver) from one computer user to another. Electronic communication systems range in scope and size:

- From a local area network electronic communication system that delivers messages within an agency or office.
- To a wide area network electronic communication system that carries messages to a variety of physical locations.
- To Internet electronic communication that allows users to send and receive messages from around the world.

- All County e-mail shall include a disclaimer as part of the e-mail signature, and shall consist of the following language that is automatically inserted by Lotus Notes / Domino server at the end of each message that is sent outside the County:

***CONFIDENTIALITY NOTICE:** This electronic communication with its contents may contain confidential and/or privileged information. It is solely for the use of the intended recipients(s). Unauthorized interception, review, use, or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, or authorized to receive for the intended recipient, please contact the sender and destroy all copies of the communication. Thank you for your consideration.*

Electronic communication **messages** are documents sent or received by a computer system. This definition includes: 1) the contents of the communication, 2) any transactional information, and 3) any attachments associated with such communication. Thus, electronic communication messages are similar to other forms of communicated messages, such as correspondence, memoranda, and circular letters.

1.8.2 Personal Use

Incidental personal use, if authorized by the appropriate department head, of the County's electronic communication system is permitted as long as it is not excessive and does not degrade the performance of services or interfere with the County's normal business practices and the performance of the County User's business tasks. County Users should exercise sound judgment and sensitivity to others when exchanging personal messages in the workplace.

Lotus Notes is the County standard e-mail system.

- All incoming e-mail must be addressed to the County User's County-supplied electronic communication address such as John.Smith@edcgov.us. firstname.lastname is the Standard Naming Convention.
- Receipt of non-County addressed e-mail via Internet based Internet Service Providers (ISP's) (jsmith@hotmail.com or comcast.com for example) is allowed; however, such email must be accessed via the Internet. Personal attachments may not be stored on County storage devices.
- Examples of County incoming e-mails include those ending with edcgov.us, co.eldorado.ca.us, edso.org, or /PV/EDC or /SLT/EDC (Lotus Notes addresses).
- The use of Internet-based commercial instant messaging products such as AOL Instant Messaging, Windows Instant Messaging, MIRC, IRC, etc. is prohibited over the County's network.
- Some electronic communication clients allow the use of downloadable plug-ins, allowing the computer user to add "emoticons" and other animations to their electronic communication. The downloading, installation and use of any of these items is prohibited on County computer systems.

1.8.3 State and Federal Laws

Use of the County's electronic communication system is subject to all applicable Federal and State communications and privacy laws. In particular, County Users need to be aware that

attaching programs, sound, video, and images to electronic communication messages may violate copyright laws, and data files containing County User or citizen information are subject to all privacy laws.

1.8.4 Restrictions

Electronic communication may not be used for:

- Unlawful activities.
- Advertising (unsolicited electronic communication commonly referred to as "Spam").
- Mail "bombs".
- Uses that violate departmental, County, State or Federal policies, such as, but not limited to, obscenity, sexual harassment, hostile work place, etc .
- Any other use which interferes with computing facilities and services of the County.

The list of restrictions is indicative rather than inclusive of restrictions and electronic communication may not be used for reasons other than those specifically mentioned.

1.8.5 False Identity

County Users shall not employ a false identity in sending electronic communication or alter forwarded electronic communication out of the context of its original meaning.

1.8.6 Representation

County Users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the County unless they are appropriately authorized, explicitly or implicitly, to do so.

1.8.7 Network Capacity

The County's electronic communication system shall not be used for purposes that could reasonably be expected to cause, either directly or indirectly, excessive use of network service or capacity, or cause interference with other County Users use of electronic communication systems, or any computing facilities or services.

For example, attaching files larger than 5 MB to an e-mail message and sending the e-mail to multiple recipients. Files meant to be shared or accessed by multiple County Users should be stored on a shared drive and a file path (link) to the file should be sent to the intended recipients.

1.8.8 Possession

County Users are not responsible for "electronic communication in their possession" when they have no "reasonable" knowledge of its existence or contents.

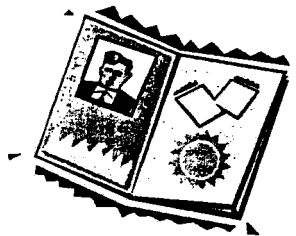
Preservation of electronic communication (subject to litigation) is required when an individual knows or should reasonably know, by official notification or other communications that the probability of litigation exists or the process of discovery pursuant to litigation exists. Electronic communication and any associated attachments shall be preserved by all reasonable means until notified in writing by County Counsel that the litigation period has

passed and that electronic communication pertaining to litigants no longer needs to be preserved. Preservation may include any and all electronic communication relating to possible litigation being copied onto readable media and delivered (with signed receipt) to County Counsel for later use. By not exercising reasonable and prudent precautions in preserving potential evidence, including electronic communication, you may subject yourself to criminal liability.

Every County User has a duty to preserve evidence in litigation. Destroying documents relevant to threatened or ongoing litigation may result in legal actions against that County User and against the County.

1.9 Use of the Internet

County User's incidental personal use of the Internet, if authorized by the appropriate department head, shall not encroach on or displace time spent performing their work duties. County Users shall not use the Internet in any way that may violate any other County rules, regulations, policies, procedures or practices, or bring civil or criminal liability or public reproach or any conduct tending to bring the County service into disrepute.



1.10 Computer User ID's and Password

All County Users shall be assigned "User ID's" and passwords. Based on a County User's responsibilities and his or her department head's authorization. The County User may be provided with access levels which allow him or her to view, create, alter, delete, print, or transmit information.

County Users are responsible for maintaining the security of their personal account passwords and may not release it for use by any other individual.

All user-level passwords (e.g., electronic communication, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months. There are some systems, such as access for DMV records, that require passwords be changed more often. Please see Section 3.2, Passwords for the correct construction of passwords.

User accounts (e.g., root, enable, NT admin, application administration accounts, etc.) that have system-level privileges or administrative privileges must have strong unique passwords (8-12 character minimum) and will face regular mandatory password changes of no more than every four (4) months.

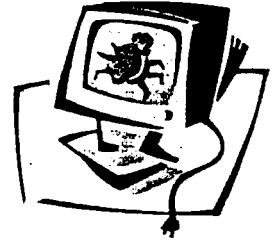
Passwords must not be inserted into electronic communication messages or other forms of electronic communication, including programming languages.

Any County User found to have violated this policy shall immediately have their access revoked and may be subject to disciplinary action.

Please see General Usage Standards and Guidelines – 3.2 Passwords in support of this policy. All user-level and system-level passwords must conform to the guidelines described in Section 3.2.1, Password Construction Guidelines.

1.11 Computer Viruses

The computer industry faces a continuing onslaught of malicious viruses, worms, malware and other damaging programs that attack computer and network resources. The County maintains equipment and software that reduces the potential impact of viruses, worms, spam, malware and phishing attacks in order to minimize impact of these invasions. It is the responsibility of the County User to take precautions to protect his/her computer and all network resources throughout the County.



Any computer or peripheral connecting to the El Dorado County network must use County approved anti-virus software. This software must be configured to receive regular software and virus signature file updates. All County computing equipment or peripherals, as applicable, shall run up to date versions of the County approved antivirus software or operating systems as approved for distribution by the I.T. department.

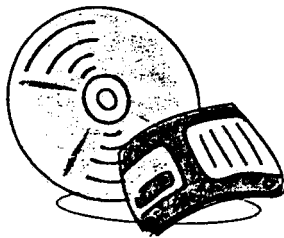
County Users should be cautious of opening electronic communication. Viruses can also be received from persons known to the recipient. If there is any doubt as to the validity of an attachment or the electronic communication, County Users shall delete the electronic communication and/or the attachment.

County Users may not download any software, including screensavers, from the Internet without prior authorization from the Director of I. T., or designee.

Computers may not simultaneously connect to the County Wide Area Network (WAN) and other networks such as commercial, private, personal or direct Internet connections via dial-up, DSL or broadband connections.

Critical data should be maintained on servers for security, anti-virus protection and to ensure data integrity through system tape back up.

All computers connecting to the County network are required to be current on all operating system, browser, Office Suite and application updates. These are the updates to the programs mentioned, not necessarily the most current release of the programs.



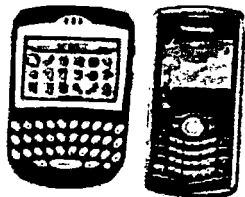
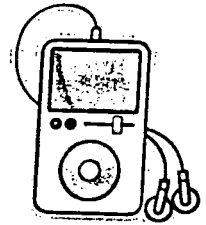
1.12 Removable Data Storage Devices

There are many forms of removable data storage devices in use today. These devices include, but are not limited to; floppy disk, CDs, DVDs, USB storage devices, MP3 players and cameras being the most common. These devices can easily spread malware (malicious software), viruses, worms, etc. to County computer equipment and network. To prevent the spread of malware

adherence to the following guidelines is required:

- Floppy drive use has been permanently discontinued.

- Data on CDs and DVDs and USB devices are automatically scanned for malware upon insertion and opening of the files contained therein.
- County digital cameras connected to County computers via docking stations pose little risk and are authorized. Personal digital cameras used in the conduct of County business are authorized to upload digital images.
- MP3 players (IPOD's, etc) may not be connected to County computing equipment. The downloading of music from the Internet to County computers is prohibited. Downloading music at home to MP3 players and connecting to County computers is prohibited due to the very high risk of infection.
- Access to "shared resource" download sites and use of software such as LimeWire and others like it using County computers is prohibited as hackers have no problems obtaining any piece of data off your computer including Personally Identifiable Information (PII). Then they can and will use this information to destroy your credit record and life as reported by all major news agencies.
- All USB based storage devices shall be equipped with integral password protected encryption or Pointsec encryption. Departments processing protected classes of information shall use Pointsec Portable Media Encryptions (PME) to protect data. Implementation of this policy shall be incremental with the acquisition of new USB devices due to budget constraints.



1.13 Portable Computing Devices (WPDA, PDA, Laptops, Tablets)

Portable computing devices such as wireless and/or standard personal digital assistants and laptop computers are subject to every element of the Computer and Network Resource Usage Policies.

Due to their portable nature they are much more prone to loss or theft. Users of these devices are required to practice due diligence in loss prevention of the physical device and data contained within.

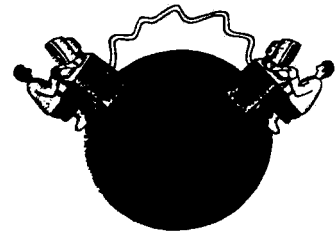
The following practices must be observed when transporting or using these devices at work or in the field:

- Physical security is one of the most important aspects of protecting these devices. Never let them out of your sight or leave them any place unattended.
- If these devices must be left in a vehicle, store them in the trunk or other secure location, camouflaging them as necessary to keep them out of sight.
- These devices should be protected with their integral security systems:
- Laptops with Biometric devices (finger print scanners, retinal scanners) or smart cards should be used whenever possible, especially equipment containing sensitive or regulatory protected data. All laptops must be equipped with Computrace theft and loss recovery software.

- Sensitive data should be stored on secured servers as much as possible. Data stored on local hard drives or portable media devices shall be encrypted and password protected.
- All portable computer devices must have appropriate County antivirus software installed and County approved firewall software for devices connecting to Internet services to protect data from hackers.
- Wireless Personal Digital Assistants may only communicate with the County e-mail system through the I.T. approved gateways into the Lotus Notes/Domino e-mail system. County approved devices include, Blackberry and Windows Mobile 5 or 6 digital assistants. Palm devices will be phased out as they reach end of life and will not be supported after that point as the gateway that supports Palm OS devices will be discontinued.
- Data from unknown sources may not be beamed to your portable devices via infrared ports.
- Devices that are lost or stolen must be immediately reported to your supervisor and I.T..

1.14 Remote Access

This policy applies to County Users utilizing remote services to access the El Dorado County network. This policy applies to all implementations of remote access that are directed through a VPN concentrator, firewall-to-firewall access, or dial-up service to access County network resources.



If approved by the appropriate department head or authorized representative (if user is not a County employee) and the County Security Officer, remote access users (County Users, outside government agencies, contractors, vendors, etc.) may utilize the benefits of remote access, which is a "user managed" service. Remote access users will be responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. When connecting to County hosted remote access services, the remote access user is responsible for any and all toll charges associated with the use of remote access equipment.

The following policies apply to remote access users:

- It is the responsibility of remote access user with remote privileges to ensure that unauthorized users are not allowed access to El Dorado County internal networks.
- When actively connected to the County network through dial-up services, all other connections to non-County networks must be disconnected.
- Remote access accounts will be created and managed by El Dorado County I.T.
- All computers connected to El Dorado County internal networks via remote access are subject to the same security requirements as those connected to the County network.

- Remote access County Users will be automatically disconnected from El Dorado County's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network.
- VPN connectivity will be through approved client software or other connectivity methods as defined by El Dorado County I.T.
- When authorized for remote access to the County network using personal equipment, County Users must understand that their machines are a de facto extension of El Dorado County's network, and as such are subject to the same rules and regulations that apply to El Dorado County-owned equipment, and their machines must be configured to comply with the security policies and standards of El Dorado County.
- When authorized for remote access to the County's network, County Users have unique access to sensitive resources. To insure network security, it is critical that all remote County Users actively support and fully comply with the measures described in these policies. Failure to comply can place the entire County network at serious risk and could lead to disciplinary action.
- Remote access users are required to complete a remote access request form, provided by I.T., which identifies security, antivirus and other computer protection requirements for the requesting party's access. The form must be signed by the department head, or authorized representative if not a County employee, and the Security Officer. After submission of the completed form, I.T. will ensure remote systems meet County specifications prior to granting access to the County network.

COUNTY USER AGREEMENT
El Dorado County Computer and
Network Policies Agreement

I have read and understand that:

- 1) As a user of the County's information technology resources, I may have access to sensitive resources that are connected through the County network. To assure security throughout the entire County network, it is critical that all users actively support and fully comply with the measures described in the Computer and Network Resource Usage Policies and Standards Guide. Failure to comply can place the entire County network at serious risk. Failure to comply may subject me to disciplinary action.
- 2) As a user of the County's information systems I shall at all times act in accordance with all applicable laws and County policies, rules or procedures. I shall not use County information technology resources in an improper or unauthorized manner.

I have received, read and am fully aware of the El Dorado County Computer and Network Resource Usage Policies and Standards Guide. I agree to comply with the terms of this policy.

User Name: _____

Signature: _____

Date: _____

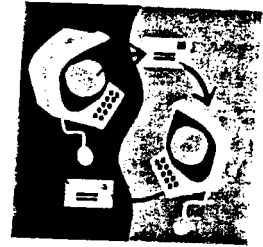
**This form shall be signed on an annual basis and be retained
in the department, district or agency file.**

GENERAL USAGE STANDARDS AND GUIDELINES

3.1 Electronic Communication

The County encourages the use of electronic communication to enhance communication and business activities. Standards are necessary to ensure the appropriate use of electronic communication and to prevent or limit disruptions to work activity and computer services.

The nature of electronic communication at the present time makes it susceptible to misuse. County Users need to be aware that sensitive or private information can be easily forwarded to other individuals the originator never intended, both internal and external to the County.



Users of the County's electronic communication services need to be aware that use of these services is a privilege granted with the expectation that it will be used for business purposes and in a professional and courteous manner similar to other forms of communication. All electronic communication sent or received by individuals through County User's accounts is the property of the County and may be examined by County officials at the request of a County User's department head and with approval from the Director of Human Resources.

It is important to understand and use electronic communication appropriately within the County use policy and your specific departmental electronic communication use policy. Additionally, for a guide to safe electronic communication use please refer to the EDCNET, the County's intranet website:

http://edcnet/IT/PUBLIC/safe_computing.html.

All e-mail, whether it is a new e-mail or it is a response, shall contain the e-mail security disclaimer as defined in Section 1.8.1 of this document.

3.1.1 Security and Confidentiality

The confidentiality of electronic communication cannot be assured. County Users should exercise extreme caution in using electronic communication to communicate confidential or sensitive material. Any electronic communication that contains protected classes of information (HIPAA, PII, PHI Sarbanes-Oxley, etc.) must be encrypted before it is electronically communicated.

3.1.2 Anti-Spam Measures

Never respond to a spam electronic communication. Many spam electronic communications may contain instructions on how to remove your address from their address list. More often than not, your response only confirms they have a valid address. They will continue to send you spam and will sell or share the now confirmed active address to other spammers.

Never use your County electronic communication account for Internet purchasing, auction sites (EBay etc.) or supply your County Internet e-mail account address to suspicious or untrusted sites.

El Dorado County has made a significant investment in technologies designed to minimize our exposure to spam and viruses. This equipment will quarantine suspicious electronic communication. The equipment uses a series of anti-spam /antivirus measures to assign a point value to incoming e-mail. When an electronic communication hits these thresholds it

is normally quarantined. Often times, incoming electronic communication may be quarantined due to poor maintenance and/or security measures at the senders end, causing their electronic communication services to be "blacklisted" and resulting in quarantine at our servers. These actions are by design and meant to protect our systems and your County computers.

The process of e-mail quarantine may delay the delivery of electronic communication. I.T. staff checks quarantine areas regularly to minimize the impact on County staff members. Although this quarantine process may at times be inconvenient, it is necessary to prevent the entry of un-wanted and potentially dangerous electronic communication into the County system.

3.1.3 HIPPA and Compliance with Electronic Communication Privacy Act

Standards are under development to comply with above regulations and acts. In general, electronic communication under the umbrella of these regulations requires data and electronic communication encryption. The County has adopted hard drive, USB portable media and e-mail encryption standards. The I.T. department will work with departments subject to these standards to ensure compliance shall be in place by July of 2010.

3.1.4 E-mail Retention

Formal e-mail retention policies are under review and will be complete in the near future; after the appropriate review and approval processes. E-mail retention policies differ from e-mail archiving. Archiving manages the size of e-mail files. Retention manages the age of e-mail and deletes e-mail that age past a certain date.

3.1.4.1 Account File Size Restrictions and E-mail Retention Standard

E-mail attachments can consume large amounts of storage space on County file servers. It is recommended that attachments be detached and stored on a local computer or stored on a server and deleted from electronic communication to preserve electronic communication server storage.

County User best practices should include proper management of their e-mail. Departments must develop guidelines pertinent to their business requirements that dictate how long specific electronic communications should be kept, what can be deleted and when. Departments undoubtedly have differing needs for retention based on Local, State, and Federal law as well as accepted best practices within their industries.

A departmental e-mail retention standard must be designed to reflect the need for each County User to manage his or her e-mail effectively and efficiently. This standard will help minimize the impact on County resources in storing and managing the County's enterprise e-mail system.

The maximum e-mail file size is set at 300 Mb. When a County User's file size reaches 250 Mb the user receives an e-mail notification that their e-mail file is reaching the maximum allowable size. If the file size reaches the 300 MB limit send\receive e-mail privileges are suspended until files are deleted or archived to bring the file size below the maximum allowable size. Contact I.T. for assistance with archiving your e-mail.

3.1.5 Managing E-mail

You may receive and manage your 'production' e-mail file and create folders as you wish and according to your department's policy.

You can manage your e-mail by:

- Deleting e-mail you no longer need.
- Saving only e-mail that you are required to save by department policy or based on legal requirements, to a designated archive folder(s). This process will move your 'archived' e-mail from your 'limited' production area to your archive storage location.
- Removing attachments from e-mail and store them on local computer and/or server storage.
- Printing your e-mail and saving the printed copy (or make Adobe 'PDFs') and then deleting the e-mail.
- Once a County User no longer needs an e-mail and moves the e-mail to the Trash folder the e-mail is held in the Trash folder for 96 hours then deleted. By deleting all e-mail in the Trash folder the County User ensures all messages are deleted. Reductions to the size of the County User e-mail account after deleting e-mails may not immediately reflect the accurate size for up to two days due to automated processes. If a County User requires the size change to take immediate effect due to reaching the 300Mb limit, contact the Help Desk.

These processes should help bring e-mail file sizes below the allowable limits.

3.1.5.1 Archiving E-mail

E-mail archiving guidelines are still under discussion at this time.

3.1.5.2 Backup Process for Production E-mail and Archived E-mail

- Production e-mail will be backed up daily (normal business day).
- Production e-mail will be backed up to tape on a weekly basis for 'off-site' disaster recovery purposes.

3.1.5.3 E-mail Account Deletions

All Internet electronic communication is forwarded to the County e-mail system, Lotus Notes. Upon notification by a department head or Human Resources that a County User is confirmed to have permanently left County service, the Internet account will be frozen or deleted. The County e-mail files are moved to "obsolete" and the County User's name is removed from the County e-mail list. Files placed in "obsolete" are retained for 60 days and then deleted. Departments requiring any deviation from this standard should immediately contact the Director of I. T. to avoid deletion of files intended for an extension of time prior to deletion.

3.1.5.4 Anti-Virus Measures and E-mail Attachments

Never open any file attached to an electronic communication from an unknown, suspicious or untrustworthy source. Delete these electronic communications immediately, then "double delete" them by emptying your Trash. One of our best lines of defense against malicious attacks is the computer user. Regularly check electronic communication for notifications sent to you by I.T. regarding viruses and electronic communication "scams". An informed computer user is an aware user and can better identify suspicious content in electronic communication.

Delete spam, chain, and other junk electronic communication without forwarding.

Never download files from unknown or suspicious sources or websites. Never visit "underground" sites, hacking sites, or any site that is not required in the execution of your duties as a County User. These sites can put the integrity of the County network at risk through malicious code, either intentionally or unintentionally.

Avoid direct disk sharing (peer to peer) with read/write access unless there is a business requirement to do so.

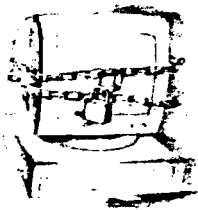
3.1.6 Electronic Communications – Instant Messaging

The County is using Lotus Instant Messaging as an additional form of electronic communication between County Users. All policies applicable to electronic mail apply to electronic messaging. Special precautions must be observed with the use of instant messaging due to the nature in which transcripts of instant messaging are logged. The default for Lotus Notes Instant Messaging is "not logged".

Should any County User receive objectionable, offensive or threatening content during an instant message session, it is important to follow these procedures:

- Do not close the instant message session or turn off your computer
- Contact your supervisor to report the behavior in question

As applicable, your supervisor will take the appropriate action, up to and including contacting the Human Resources department who will direct the collection of the data in question, following strict confidentiality guidelines.



3.2 Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of El Dorado County's entire corporate network. As such, all El Dorado County Users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this standard is to establish criteria for creation of strong passwords, the protection of those passwords, and the frequency of change. This includes all County Users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any El Dorado County facility, has access to the County network, or stores any non-public County information.

3.2.1 Password Construction Guidelines

Passwords are used for various purposes in El Dorado County. Some of the more common uses include: personal computer accounts, network server accounts, web accounts, electronic communication accounts, screen saver protection, voice electronic communication password, and mainframe accounts.

Poor or weak passwords have the following characteristics:

- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "El Dorado County", "County", "EDC", or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong or effective passwords have the following characteristics:

- The password contains at LEAST 8 characters.
- The password contains both upper and lower case characters (e.g., a-z, A-Z)
- The password has digits and punctuation characters as well as letters (e.g., 0-9, ! @ # \$ % ^ & * () _ + | ~ - = \ ` { } [] : " ; ' < > ? , . /)
- The password is not a word in any language, slang, dialect, jargon, etc.
- The password is not based on personal information, names of family, etc.

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do **NOT** use either of the above examples as passwords!

3.2.2 Password Protection Standards

Do not use the same password for El Dorado County accounts as for other non-County access (e.g., personal ISP account, EBay, personal electronic communication accounts, etc.). Do not share El Dorado County passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential County information.

Here is a list of password "don'ts":

- Don't reveal a password over the phone to un-authorized personnel.

- Don't reveal a password in an electronic communication message.
- Don't reveal a password to the manager without a written request for such information from your manager.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on vacation.
- Don't use the "Remember Password" feature of applications (e.g., Internet Explorer, Outlook, Outlook Express, and Entourage).
- Don't write passwords down and store them anywhere in your office.
- Don't store passwords in a file on ANY computer system (including PDA's) without encryption.

All computing equipment deployed in El Dorado County shall have screen savers with password protection enabled and set to lock the computer after ten (10) minutes of inactivity. County Users should hit "Ctrl/Alt/Delete keys and lock their computers to protect against un-authorized access whenever leaving their work station.

If someone demands a password, refer them to this document or have them call the Director of I. T.. Departments needing authorized access should contact the Information Technology department to securely address this need.

If an account or password is suspected to have been compromised, report the incident to I.T. immediately and change all passwords.

3.2.3 Application Development Password Standards

Mainframe applications should use RACF security functionality. Client-server and web-based applications should use Active Directory Services security functionality.

3.2.4 Pass Phrases

Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.

Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is more secure against "dictionary attacks."

A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good pass phrase:

"TheTrafficOn50WasTerribleThisMorning"

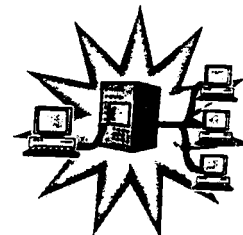
All of the rules above that apply to passwords apply to pass phrases.

3.2.5 Use of Passwords and Pass Phrases for Remote Access Users

Access to the El Dorado County networks via Virtual Private Networking (VPN) access and some networked resources are controlled using the username/password (challenge/response) mode of authentication. Access to the County network via VPN is tightly controlled.

3.3 Server Storage Utilization

To maximize server storage, County Users should properly manage their data and directory structures. There are several methods of file storage and associated back-up. The recommendations in the next section provide options and recommendations for file storage, directory structure and back-ups to ensure the availability of server storage space.



3.3.1 File Storage Options

- Operating system and applications are loaded on the desktop computer and all data files stored on the local machine hard drive. *This option provides local access to the computer data files, but offers no backup of those files. Hard drive failure will result in complete loss of data files. **This option is not recommended.***
- Operating system and applications are loaded locally and all data files are stored on a network server. *This option safeguards data in two ways: 1) data files reside on servers, 2) data files on servers are backed up to tape nightly. A possible drawback to this option is the inability to access data on the server in the event of server or network problems.*
- Operating system and applications are loaded locally. All data files are stored on the local hard drive and its directory structure configured to allow for scheduled copying of local data files to the server. *This option safeguards data in three ways: 1) data files reside on local drives, 2) data files reside on server hard drives, 3) data files are backed up to tape nightly. In the event of network or server problems, data files stored locally will be available. While this method requires the largest amount of user intervention due to regularly scheduled backups of local data files to server drives, it does provide maximum availability and protection of data files.*
- "Thin Client" computer; all files reside on a server. The operating system and applications run at the server level, data files are stored on server drives. Proper file management at the server level preserves hard drive space.

3.3.2 Server File Storage

- The majority of County computers are connected to Windows based servers. These servers store data files and send print jobs to networked printers. Storage must be managed to maximize storage capacity.

- Server hard drive arrays have finite capacity. NEVER copy the entire contents of local drives to server drives. This wastes server-based storage.
- County User-specific data files should be copied only to the County User's server home directory which is normally designated as the "H:" drive.
- Data files common to a group should only be copied to the "shared" server directory's appropriate sub-directory. Always store data files in the appropriate sub-directory as defined within your department and/or group. NEVER store data files at the root of shared directories.
- Do not store multiple copies of data files on a server. There is no need to have a copy of the same file in your home directory and a group directory. Do not decompress operating system or application service packs or updates to server hard drives.
- Clean up your directories at least monthly. Delete old data files or files no longer needed and remove unnecessary iterations or versions of data files. Server storage is not to be used for storing non-work-related music, video, or picture files.

EXHIBIT C

PATIENT CONSENT FORM

**Clinicians Telemed Medical Group, Inc.
Authorization and Consent to Participate in
Telemedicine Consultation**

Patient Name: _____ Patient ID #: _____

1. **PURPOSE:** The purpose of this form is to obtain your consent to participate in a telemedicine consultation in connection with the following procedure(s):
2. **NATURE OF TELEMED CONSULTATION:** During the telemedicine consultation:
 - a. Details of your medical history, examinations, x-rays, and tests will be discussed with other health professionals through the use of digital images and email.
 - b. Physical examination may take place
 - c. Video and/or photo recordings may be taken of the procedure(s)
3. **MEDICAL INFORMATION AND RECORDS:** All existing laws regarding your access to medical information and copies of your medical records apply to this digital imaging consultation. Additionally, dissemination of any patient identifiable images or other information from this digital imaging interaction shall not occur without your consent.
4. **CONFIDENTIALITY:** Reasonable and appropriate efforts have been made to eliminate any confidentiality risks associated with the digital imaging consultation, and all existing confidentiality protections under federal and California law apply to information disclosed during this digital imaging consultation.
5. **RIGHTS:** You may withhold or withdraw consent to the digital imaging consultation at any time before or during the consultation without affecting the right to future care or treatment.
6. **DISPUTES:** I agree that any disputes I may have with any medical provider arising from this digital imaging consultation will be resolved in California and that California law shall apply to any such disputes.
7. **RISKS, CONSEQUENCES AND BENEFITS:** I have been advised of all the potential risks, consequences and benefits of digital imaging. My health care practitioner has discussed with me the information provided above. I have had an opportunity to ask questions about this information and all of my questions have been answered. I understand the written information provided above.

Signature: _____
Patient or patient's legal representative

Date: _____

EXHIBIT D

STATE REQUIRED TERMS AND CONDITIONS

1. Utilization Review/Quality Assurance

Contractor shall establish and maintain systems to review the quality and appropriateness of services in accordance with applicable Federal and State statutes and regulations and guidelines operative during the term of this Agreement.

The California Department of Mental Health (DMH) may review the existence and effectiveness of any utilization review systems of the Contractor as necessary.

2. Assurances

Contractor shall provide services in accordance with all applicable Federal and State statutes and regulations.

3. Cost Report

The Contractor shall submit a fiscal year-end cost report, due to DMH no later than December 31 following the close of the fiscal year, in accordance with W&I Section 5651(a)(4), 5664(a) and (b), 5705(b)(3), 5718(c) and guidelines established by DMH.

4. DMH -Special Terms and Conditions

California Department of Mental Health Exhibit D-1, Special Terms and Conditions, is hereby incorporated by reference as if fully set forth herein. By signing this Agreement, Contractor agrees to comply with all these provisions incorporated hereto.

California Department of Mental Health Exhibit D-2, Confidentiality and Information Security Provisions, is hereby incorporated by reference as if fully set forth herein. By signing this Agreement, Contractor agrees to comply with all these provisions incorporated hereto.

5. NON-DISCRIMINATION CLAUSE

a. During the performance of this Agreement, Contractor and its subcontractors shall not unlawfully discriminate, harass, or allow harassment against any employee or applicant for employment because of sex, race, color, ancestry, religious creed, national origin, physical disability (including HIV and AIDS), mental disability, medical condition (cancer), age (over 40), marital status, and denial of family care leave. Contractor and subcontractors shall insure that the evaluation and treatment of their employees and applicants for employment are free from such discrimination and harassment. Contractor and subcontractors shall comply with the provisions of the Fair Employment and Housing Act (Gov. Code §12990 (a-f) et seq.) and the applicable regulations promulgated thereunder (California Code of Regulations, Title 2, Section 7285 et seq.). The applicable regulations of the Fair Employment and Housing Commission implementing Government Code Section 12990 (a-f), set forth in Chapter 5 of Division 4 of Title 2 of the California Code of Regulations, are incorporated into this Agreement by reference and made a part hereof as if set forth in full. Contractor and its subcontractors shall give written notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other Agreement.

b. Consistent with the requirements of applicable federal or state law, the Contractor shall not engage in any unlawful discriminatory practices in the admission of beneficiaries, assignments of accommodations, treatment, evaluation, employment of personnel, or in any other respect on the basis of race, color, gender, religion, marital status, national origin, age, sexual preference or mental or physical handicap.

c. The Contractor shall comply with the provisions of Section 504 of the Rehabilitation Act of 1973, as amended, pertaining to the prohibition of discrimination against qualified handicapped persons in all federally assisted programs or activities, as detailed in regulations signed by the Secretary of Health and Human Services, effective June 2, 1977, and found in the Federal Register, Volume 42, No. 86, dated May 4, 1977.

d. Notwithstanding other provisions of this section, the Contractor may require a determination of medical necessity pursuant to Title 9, CCR, Section 1820.205, Section 1830.205 or Section 1830.210, prior to providing covered services to a beneficiary.

e. Contractor shall include the nondiscrimination and compliance provisions of this clause in all subcontracts to perform work under the Agreement.

6. AUDIT

Contractor agrees that the awarding department, the Department of General Services, the Bureau of State Audits, the Auditor General, or their designated representative shall have the right to review and to copy any records and supporting documentation pertaining to the performance of this Agreement. Contractor agrees to maintain such records for possible audit for a minimum of three (3) years after final payment, unless a longer period of records retention is stipulated. Contractor agrees to allow the auditor(s) access to such records during normal business hours and to allow interviews of any employees who might reasonably have information related to such records. Further, Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Agreement. (Gov. Code §8546.7, Pub. Contract Code §10115 et seq., CCR Title 2, Section 1896).

7. Transfer of Care

Prior to the termination or expiration of this contract and upon request by the DMH, the Contractor shall assist the State in the orderly transfer of beneficiaries' mental health care. In doing this, the Contractor shall make available to the DMH copies of medical records, patient files, and any other pertinent information, including information maintained by any subcontractor, necessary for efficient case management of beneficiaries, as determined by the DMH. Costs of reproduction shall be borne by the DMH. In no circumstances shall a beneficiary be billed for this service.

8. Inspection Rights

- a. The Contractor shall allow the DMH, California Department of Health Care Services (DHS), California Health and Human Services Agency (HSS), the Comptroller General of the United States, and other authorized federal and state agencies, or their duly authorized representatives, to inspect or otherwise evaluate the quality, appropriateness, and timeliness of services performed under this contract, and to inspect, evaluate, and audit any and all books, records, and facilities maintained by the Contractor and subcontractors, pertaining to such services at any time during normal business hours. Books and records include, but are not limited to, all physical records originated or prepared pursuant to the performance under this contract including working papers, reports, financial records and books of account, beneficiary records, prescription files, subcontracts, and any other documentation pertaining to covered services and other related services for beneficiaries. Upon request, at any time during the period of this contract, the Contractor shall furnish any such record, or copy thereof, to the DMH, DHS, or HHS. Authorized agencies shall maintain the confidentiality of such books and records in accordance with applicable laws and regulations.
- b. The Contractor agrees to make all of its books and records, pertaining to the goods and services furnished under the terms of the Agreement, available for inspection, examination or copying by the DMH, DHS, HHS, the Comptroller General of the United States, and other authorized federal and state agencies, or their duly authorized representatives, at all reasonable times at the Contractor's place of business or at such other mutually agreeable location in California, in a form maintained in accordance with the general standards applicable to such book or record keeping, for a term of at least five years from the close of the DMH's fiscal year in which the subcontract was in effect.
- c. The Contractor agrees to include in any subcontractor's agreement the requirement to make all of its books and records, pertaining to the goods and services furnished under the terms of the subcontract, available for inspection, examination or copying by the DMH, DHS, HHS, the Comptroller General of the United States, and other authorized federal and state agencies, or their duly authorized representatives, at all reasonable times at the subcontractor's place of business or at such other mutually agreeable location in California, in a form maintained in accordance with the general standards applicable to such book or record keeping, for a term of at least five years from the close of the DMH's fiscal year in which the subcontract was in effect.

9. Additional Contract Provisions

- a. The Contractor shall comply with the provisions of the Copeland Anti-Kickback Act (18 U.S.C. 874 and 40 U.S.C. 276c), which requires that all contracts and subcontracts in excess of \$2,000 for construction or repair awarded by the Contractor and its subcontractors shall include a provision for compliance with the Copeland Anti-Kickback Act (18 U.S.C. 874), as supplemented by Department of Labor regulations (Title 29, CFR, Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in part by Loans or Grants from the United States").
- b. The Contractor shall comply with the provisions of Davis-Bacon Act, as amended (40 U.S.C. 276a to a-7), which requires that, when required by Federal Medicaid program legislation, all construction contracts awarded by the Contractor and its subcontractors of more than \$2,000 shall include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 276a to a-7) as supplemented by Department of Labor regulations (Title 29, CFR, Part 5, "Labor Standards Provisions Applicable to Contracts Governing Federally Financed and Assisted Construction").

c. The Contractor shall comply with the provisions of the Contract Work Hours and Safety Standards Act (40 U.S.C. 327-333), as applicable, which requires that all subcontracts awarded by the Contractor in excess of \$2,000 for construction and in excess of \$2,500 for other subcontracts that involve the employment of mechanics or laborers shall include a provision for compliance with sections 102 and 107 of the Contract Work Hours and Safety Standards Act (40 U.S.C. 327-333), as supplemented by Department of Labor regulations (Title 29, CFR, Part 5).

d. The Contractor shall comply with the provisions of Clean Air Act (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), as amended, which provide that contracts and subcontracts of amounts in excess of \$100,000 shall contain a provision that requires the Contractor or subcontractor to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act. Violations shall be reported to the Centers for Medicare and Medicaid Services.

e. The Contractor shall comply with the provisions of Title 42, CFR, Section 438.610 and Executive Orders 12549 and 12689, "Debarment and Suspension," which excludes parties listed on the General Services Administration's list of parties excluded from federal procurement or nonprocurement programs from having a relationship with the Contractor.

f. The Contractor shall not employ or contract with providers or other individuals and entities excluded from participation in Federal health care programs under either Section 1128 or 1128A of the Social Security Act. Federal financial participation is not available for amounts expended for providers excluded by Medicare, Medicaid, or the State Children's Insurance Program, except for emergency services.

10. Inpatient Contracts and Subcontracts

If this contract is for inpatient services, the Contractor acknowledges that they must maintain necessary licensing and certification. All inpatient subcontracts must require that subcontractors maintain necessary licensing and certification.

11. Assignment or Delegation

Contractor agrees that assignment or delegation of this Agreement shall be void, unless prior written approval is obtained from County.

12. Hold Harmless

Contractor agrees to hold harmless both the State and beneficiaries in the event the County cannot or shall not pay for services performed by the Contractor pursuant to this Agreement.

13. Additional Requirements Based on Federal Regulations

If applicable, based on the services provided under this Agreement, the Contractor agrees to comply with:

a. The Contractor shall maintain written policies and procedures respecting advance directives in compliance with the requirements of Title 42, Code of Federal Regulations (CFR), Sections 422.128 and 438.6(i)(1), (3) and (4). Any written materials prepared by the Contractor for beneficiaries shall be updated to reflect changes in state laws governing advance directives as soon as possible, but no later than 90 days after the effective date of the change.

b. The Contractor shall obtain approval from the DMH prior to implementing a Physician Incentive Plan as described at Title 42, CFR, Section 438.6(h). The DMH shall approve the Contractor's request only if the proposed Physician Incentive Plan complies with all applicable federal and state regulations.

EXHIBIT D-1 rev Mar 2008
CALIFORNIA DEPARTMENT OF MENTAL HEALTH
SPECIAL TERMS AND CONDITIONS

1. **SUBCONTRACTS.** Except for subcontracts identified in the proposal in accordance with the Request for Proposal or Invitation for bid, Contractor shall submit any subcontracts which are proposed to be entered into in connection with this Contract to the State Agency (State) for its prior written approval before entering into the same. No work shall be subcontracted without the prior written approval of the State. Upon the termination of any subcontract, State shall be notified immediately. Any subcontract shall include all the terms and conditions of this Contract and its attachments.

2. **PUBLICATIONS AND REPORTS.**

If a publication and/or report is required under this Contract, Contractor shall:

- A. Incorporate any comments or revisions required by the State into any publication or report and shall not publish any material until it receives final State approval.
- B. Furnish two copies of each publication and report required plus one reproducible original.
- C. Prepare all illustrations, maps and graphs in a manner which allows the complete illustration to be contained on a single 8-1/2 by 11 page unless specific written approval is given to the contrary.
- D. Print all graphs, illustrations and printed materials in a single color throughout each publication unless prior State approval is granted.
- E. Place the Contractor's name only on the cover and title page of publications and reports and summaries. Covers and title pages shall read as follows:

DEPARTMENT OF MENTAL HEALTH
TITLE
By (Contractor)

The State reserves the right to use and reproduce all publications, reports, and data produced and delivered pursuant to this Contract. State further reserves the right to authorize others to use or reproduce such materials, provided the author of the report is acknowledged in any such use or reproduction.

If the publication and/or report are prepared by non-employees of the State, and the total cost for such preparation exceeds \$5,000, the publication and/or report shall contain the numbers and dollar amounts of all contracts and subcontracts relating to the preparation of the publication and report in a separate section of the report (Government Code Section 7550).

3. **PROGRESS REPORTS.** If progress reports are required by the Contract, Contractor shall provide a progress report in writing, or orally if approved by the State Contract Manager, at least once a month to the State Contract Manager. This progress report shall include, but not limited to, a statement that the Contractor is or is not on schedule, any pertinent reports, or interim findings. Contractor shall cooperate with and shall be available to meet with the State to discuss any difficulties, or special problems, so that solutions or remedies can be developed as soon as possible.
4. **PRESENTATION.** Upon request, Contractor shall meet with the State to present any findings, conclusions, and recommendations required by the Contract for approval. If set forth in the Contract, Contractor shall submit a comprehensive final report for approval. Both the final meeting and the final report shall be completed on or before the date indicated in the Contract.
5. **DEPARTMENT OF MENTAL HEALTH STAFF.** Department of Mental Health staff shall be permitted to work side by side with Contractor's staff to the extent and under conditions as directed by the State Contract Manager. In this connection, Department of Mental Health staff shall be given access to all data, working papers, etc., which Contractor seeks to utilize.
6. **CONFIDENTIALITY OF DATA AND DOCUMENTS.**

Contractor shall not disclose data or documents or disseminate the contents of the final or any preliminary report without written permission of the State Contract Manager. However, all public entities shall comply with California Public Records Act (Government Code Sections 6250 et seq.) and the Freedom of Information Act (Title 5 of the United States Code Section 552), as applicable.

Permission to disclose information or documents on one occasion shall not authorize Contractor to further disclose such information or documents on any other occasions except as otherwise provided in the Contract or required by law.

Contractor shall not comment publicly to the press or any other media regarding the data or documents generated, collected, or produced in connection with this contract, or the State's actions on the same, except to the Department of Mental Health staff, Contractor's own personnel involved in the performance of this Contract, or as required by law.

If requested by State, Contractor shall require each of its employees or officers who will be involved in the performance of this Contract to agree to the above terms in a form to be approved by State and shall supply State with evidence thereof.

Each subcontract shall contain the foregoing provisions related to the confidentiality of data and nondisclosure.

After any data or documents submitted has become a part of the public records of the State, Contractor may at its own expense and upon written approval by the State Contract Manager, publish or utilize the same data or documents but shall include the following Notice:

LEGAL NOTICE

This report was prepared as an account of work sponsored by the Department of Mental Health (Department), but does not necessarily represent the views of the Department or any of its employees except to the extent, if any, that it has formally been approved by the Department. For information regarding any such action, communicate directly with the Department at P.O. Box 952050, Sacramento, California, 94252-2050. Neither said Department nor the State of California, nor any officer or employee thereof, or any of its contractors or subcontractors makes any warranty, express or implied, or assumes any legal liability whatsoever for the contents of this document. Nor does any party represent that use of the data contained herein, would not infringe upon privately owned rights without obtaining permission or authorization from any party who has any rights in connection with the data.

7. PROVISIONS RELATING TO DATA.

"Data" as used in this Contract means recorded information, regardless of form or characteristics, of a scientific or technical nature. It may, for example, document research, experimental, developmental or engineering work; or be usable or be used to define a design or process; or support a premise or conclusion asserted in any deliverable document called for by this Contract. The data may be graphic or pictorial delineations in media, such as drawings or photographs, charts, tables, mathematical modes, collections or extrapolations of data or information, etc. It may be in machine form, as punched cards, magnetic tape, computer printouts, or may be retained in computer memory.

"Generated data" is that data, which a Contractor has collected, collated, recorded, deduced, read out or postulated for utilization in the performance of this Contract. Any electronic data processing program, model or software system developed or substantially modified by the Contractor in the performance of this Contract at State expense, together with complete documentation thereof, shall be treated in the same manner as generated data.

"Deliverable data" is that data which under terms of this Contract is required to be delivered to the State. Such data shall be property of the State.

Prior to the expiration of any legally required retention period and before destroying any data, Contractor shall notify the State of any such contemplated action; and State may within 30 days of said notification determine whether or not this data shall be further preserved. The State shall pay the expense of further preserving this data. State shall have unrestricted reasonable access to the data that is preserved in accordance with this Contract.

Contractor shall use best efforts to furnish competent witnesses to identify such competent witnesses to testify in any court of law regarding data used in or generated under the performance of this Contract.

8. APPROVAL OF PRODUCT. Each product to be approved under this Contract shall be approved by the Contract Manager. The State's determination as to satisfactory work shall be final absent fraud or mistake.
9. SUBSTITUTIONS. Contractor's key personnel as indicated in its proposal may not be substituted without Contract Manager's prior written approval.
10. NOTICE. Notice to either party shall be given by first class mail properly addressed, postage fully prepaid, to the address beneath the name of each respective party. Such notice shall be effective when received as indicated by post office records or if deemed undeliverable by post office, such notice shall be effective nevertheless 15 days after mailing. Alternatively, notice may be given by personal delivery by any means whatsoever to the party, and such notice shall be deemed effective when delivered.
11. WAIVER. No waiver of any breach of this Contract shall be held to be a waiver of any other or subsequent breach. All remedies afforded in this Contract shall be taken and construed as cumulative; that is, in addition to every other remedy provided therein or by law. The failure of State to enforce at any time the provisions of this Contract, or to require at any time performance by the Contractor of any of the provisions, shall in no way be construed to be a waiver of such provisions not to affect the validity of this Contract or the right of State to enforce said provisions.

12. **GRATUITIES AND CONTINGENCY FEES.** The State, by written notice to the Contractor, may terminate the right of Contractor to proceed under this Contract if it is found, after notice and hearing by the State, that gratuities were offered or given by the Contractor or any agent or representative of the Contractor to any officer or employee of the State with a view toward securing a contract or securing favorable treatment with respect to the awarding, amending, or performing of such contract.

In the event this Contract is terminated as provided in the paragraph above, State shall be entitled (a) to pursue the same remedies against Contractor as it could pursue in the event of the breach of the Contract by the Contractor, and (b) as a predetermined amount of liquidated damages, to exemplary damages in an amount which shall not be less than three times the cost incurred by the Contractor in providing any such gratuities to any such officer or employee.

The rights and remedies of the State provided in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

The Contractor warrants by execution of this Contract that no person or selling agency has been employed or retained to solicit or secure this Contract upon a Contract or understanding for a commission, percentage, brokerage or contingent fee, excepting bona fide employees of Contractor, for the purpose of securing business. For breach or violation of this warranty, the State shall have the right to annul this Contract without liability, paying only for the values of the work actually returned, or in its discretion to deduct from the contract price or consideration, or otherwise recover, the full amount of such commission, percentage, brokerage, or contingent fee.

13. **INSURANCE.** Contractor hereby warrants that it carries and shall maintain in full force and effect during the full term of this contract and any extensions to said term:

Sufficient and adequate Worker's Compensation Insurance for all of its employees who shall be engaged in the performance of this Contract and agrees to furnish to State satisfactory evidence thereof at any time the State may request the same; and

Sufficient and adequate Liability Insurance to cover any and all potential liabilities and agrees to furnish to State satisfactory evidence thereof upon request by State.

14. **CONTRACT IS COMPLETE.** Other than as specified herein, no document or communication passing between the parties hereto shall be deemed a part of this Contract.
15. **CAPTIONS.** The clause headings appearing in this Contract have been inserted for the purpose of convenience and ready reference. They do not purport to and shall not be deemed to define, limit or extend the scope or intent of the clauses to which they pertain.
16. **PUBLIC HEARINGS.** If public hearings on the subject matter dealt with in this Contract are held within one year from the contract expiration date, Contractor shall make available to testify the personnel assigned to this Contract at the hourly rates specified in the Contractor's proposed budget. State shall reimburse Contractor for travel of said personnel at the contract rates for such testimony as may be requested by State.
17. **DVBE.** Unless specifically waived by the Deputy Director of Administrative Services of the Department, Contractor shall comply with the Disabled Veteran Business Enterprises participation goal in accordance with the provisions of Public Contract Code Section 10115 et seq.
18. **FORCE MAJEURE.** Neither the State nor the Contractor shall be deemed to be in default in the performance of the terms of this Contract if either party is prevented from performing the terms of this Contract by causes beyond its control, including without being limited to: acts of God, interference, rulings or decision by municipal, Federal, State or other governmental agencies, boards or commissions; any laws and/or regulations of such municipal, State, Federal, or other governmental bodies; or any catastrophe resulting from flood, fire, explosion, or other causes beyond the control of the defaulting party. If any of the stated contingencies occur, the party delayed by force majeure shall immediately give the other party written notice of the cause of delay. The party delayed by force majeure shall use reasonable diligence to correct the cause of the delay, if correctable, performance under this Contract.
19. **PERMITS AND LICENSES.** The Contractor shall procure and keep in full force and effect during the term of this Contract all permits, registrations and licenses necessary to accomplish the work specified in this Contract, and give all notices necessary and incident to the lawful prosecution of the work.
20. The Contractor shall keep informed of, observe, comply with, and cause all of its agents and employees to observe and to comply with all prevailing Federal, State, and local laws, and rules and regulations made pursuant to said Federal, State, and local laws, which in any way affect the conduct of the work of this Contract. If any conflict arises between provisions of the plans and specifications and any such law above referred to, then the Contractor shall immediately notify the State in writing.
21. **LITIGATION.** The State, promptly after receiving notice thereof, shall notify the Contractor in writing of the commencement of any claim, suit, or action against the State or its officers or employees for which the contractor

must provide indemnification under this Contract. The failure of the State to give such notice, information, authorization or assistance shall not relieve the Contractor of its indemnification obligations. The Contractor shall immediately notify the State of any claim or action against it which affects, or may affect, this Contract, the terms and conditions hereunder, or the State, and shall take such action with respect to said claim or action which is consistent with the terms of this Contract and the interest of the State.

22. **DISPUTES.** Contractor shall first discuss and attempt to resolve any dispute arising under or relating to the performance of this Contract, which is not disposed of by the Contract, informally with the State Contract Manager. If the dispute cannot be disposed of at this level, then the dispute shall be decided by the Department of Mental Health's Deputy Director of Administration. All issues pertaining to this dispute shall be submitted in written statements and addressed to the Deputy Director of Administration, Department of Mental Health, 1600 9th Street, Room 150, Sacramento, California 95814. Such written notice must contain the Contract Number. The decision of the Deputy Director of Administrative Services shall be final and binding to all parties. Within ten days of receipt of the written grievance report from the Contractor, the Deputy Director of Administration Director of Administration or his/her designee, the Contractor shall proceed diligently with the performance of the Contract. Neither the pendency of a dispute, nor its consideration by the Deputy Director of Administration, shall excuse the Contractor from full and timely performance of the services required in accordance with the terms of the contract.
23. Notwithstanding any other provisions of this Contract, after recourse to the procedure set forth in the paragraph above, any controversy or claim arising out of or relating to this Contract or breach thereof shall be settled by arbitration at the election of either party in accordance with California Public Contract Code Section 10240 et. seq. and judgment upon the award rendered by the arbitration may be entered in any court having jurisdiction thereof.
24. **EVALUATION OF CONTRACTOR'S PERFORMANCE.** The Contractor's performance under this Contract shall be evaluated by the State after completion of the contract. A copy of the written evaluation shall be maintained in the contract file and may be submitted to the Office of Legal Services, Department of General Services.
25. **TRAVEL.** Contractor's headquarters for purposes of payment of travel shall be the city designated in the signature block unless otherwise specified in the contract.
26. For travel necessary to the performance of this Contract, contractor shall use and submit travel reimbursement forms provided by the Department . All reimbursements shall be made in accordance with, and shall not exceed the rates authorized by, the State Administrative Manual and the Policies and Procedures of the Department. All requests to exceed any base reimbursement rate established in the State Administrative Manual or the Policies and Procedures of the Department must be made and approved prior to the date of travel and must be submitted in writing to the State's Contract Manager.
27. **TERMINATION.** Unless otherwise specified, either party may terminate this Contract by giving 30 days written notice to the other party. The notice of termination shall specify the effective date of termination. Upon the Contractor's receipt of notice of termination from the State, and except as otherwise directed in the notice, the Contractor shall:
 - A. Stop work on the date specified in the notice.
 - B. Place no further orders or enter into any further subcontracts for materials, services or facilities except as necessary to complete work under the Contract up to effective date of termination.
 - C. Terminate all orders and subcontracts;
 - D. Promptly take all other reasonable and feasible steps to minimize any additional cost, loss, or expenditure associated with work terminated, including, but not limited to reasonable settlement of all outstanding liability and claims arising out of termination of orders and subcontracts;
 - E. Deliver or make available to the Department all data, drawings, specifications, reports, estimates, summaries, and such other information and materials as may have been accumulated by the Contractor under this Contract, whether completed, partially completed, or in progress.

In the event of termination, an equitable adjustment in the price provided for this Contract shall be made. Such adjustment shall include reasonable compensation for all services rendered, materials supplies, and expenses incurred pursuant to this Contract prior to the effective date of termination.
28. **CONFIDENTIALITY AND INFORMATION SECURITY PROVISIONS.** The Contractor shall comply with applicable laws and regulations, including but not limited to Sections 14100.2 and 5328 et seq. of the Welfare and Institutions Code, Section 431.300 et seq. of Title 42, Code of Federal Regulations, and the Health Insurance Portability and Accountability Act (HIPAA), and it's implementing regulations (including but not limited to Title 45, CFR, Parts 160, 162 and 164) regarding the confidentiality and security of individually identifiable health information (IIHI).
29. **NONDISCLOSURE.** Contractor shall not use or disclose confidential, individually identifiable, or sensitive information other than as permitted or required by the Contract and as required by law.

30. AUDITS, INSPECTION AND ENFORCEMENT.

- A. From time to time, the State may inspect the facilities, systems, books and records of Contractor to monitor compliance with the Contract.
- B. Contractor shall promptly remedy any violation of any provision of the Contract and shall certify the same to the Department Information Security Officer in writing.
- C. The fact that the State 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 the Contract.
- D. The State's failure to detect or the State's detection of any unsatisfactory practices, but failure to notify Contractor or require Contractor's remediation of the unsatisfactory practices does not constitute acceptance of such practice or a waiver of the State's enforcement rights under the Contract.

31. Use of State Funds. Contractor, including its officers and members, shall not use funds received from the Department pursuant to this contract to support or pay for costs or expenses related to the following:

- A. Campaigning or other partisan activities to advocate for either the election or defeat of any candidate for elective office, or for or against the passage of any proposition or ballot measure; or,
- B. Lobbying for either the passage or defeat of any legislation.

This provision is not intended and shall not be construed to limit any expression of a view, opinion, or position of any member of Contractor as an individual or private citizens, as long as state funds are not used; nor does this provision limit Contractor from merely reporting the results of a poll or survey of its membership.

32. Drug-Free Workplace Certification. Contractor shall comply with the requirements of the Drug-Free Workplace Act of 1990 (Government Code Section 8350 et seq.) and shall provide a drug-free workplace.

33. Conflict of Interest Certification. In accordance with State laws and Departmental policy, no employees (including contractors) shall participate in incompatible activities, which are in conflict with their job duties. In addition, State law requires employees whose positions are designated in the Department's Conflict of Interest Code to file statements of economic interest. Employees whose positions have been designated will be notified by the Department if a statement is required.

In signing this contract, I certify that I have read and understand GOVERNMENT CODE 19990.

EXHIBIT D-2 rev Mar 2008
CALIFORNIA DEPARTMENT OF MENTAL HEALTH
CONFIDENTIALITY AND INFORMATION SECURITY PROVISIONS

1. CONFIDENTIALITY AND INFORMATION SECURITY PROVISIONS.

A. The Contractor shall comply with applicable laws and regulations, including but not limited to Sections 14100.2 and 5328 et seq. of the Welfare and Institutions Code, Section 431.300 et seq. of Title 42, Code of Federal Regulations, and the Health Insurance Portability and Accountability Act (HIPAA), including but not limited to Section 1320 d et seq. of Title 42, United States Code and its implementing regulations (including but not limited to Title 45, CFR, Parts 142, 160, 162 and 164) regarding the confidentiality and security of individually identifiable health information (IIHI).

B. Permitted Uses and Disclosures of IIHI by the Contractor.

1) *Permitted Uses and Disclosures.* Except as otherwise provided in this Agreement, the Contractor, may use or disclose IIHI to perform functions, activities or services identified in this Agreement provided that such use or disclosure would not violate federal or state laws or regulations.

2) *Specific Uses and Disclosures Provisions.* Except as otherwise indicated in the Agreement, the Contractor may:

a) Use and disclose IIHI for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor, provided that such use and disclosures are permitted by law.

b) Use IIHI to provide data aggregation services to DMH. Data aggregation means the combining of IIHI created or received by the Contractor for the purposes of this contract with IIHI received by the Contractor in its capacity as the Contractor of another HIPAA covered entity, to permit data analyses that relate to the health care operations of DMH.

C. Safeguards. Contractor shall develop and maintain an information privacy and security program that includes the implementation of administrative, technical, and physical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities. The information privacy and security program shall reasonably and appropriately protect the confidentiality, integrity, and availability of the IIHI that it creates, receives, maintains, or transmits; and prevent the use or disclosure of IIHI other than as provided for by this Agreement. The Contractor shall provide DMH with information concerning such safeguards as DMH may reasonably request from time to time.

The Contractor shall implement administrative, technical, and physical safeguards to ensure the security of DMH information on portable electronic media (e.g., floppy disks and CD-Rom) and in paper files. Administrative safeguards to be implemented shall include, but are not limited to training, instructions to employees, and policies and procedures regarding the HIPAA Privacy Rule. Technical safeguards to be implemented shall include, but are not limited to, role based access, computer passwords, timing out of screens, storing laptop computers in a secure location (never leaving the equipment unattended at workplace, home or in a vehicle) and encryption. Physical safeguards to be implemented shall include, but are not limited to, locks on file cabinets, door locks, partitions, shredders, and confidential destruct.

D. The Contractor shall implement appropriate authentication methods to ensure information system access to confidential, personal (e.g., IIHI) or sensitive data is only granted to properly authenticated and authorized persons. If passwords are used in user authentication (e.g., username/password combination), the Contractor shall implement strong password controls on all compatible computing systems that are consistent with the National Institute of Standards and Technology (NIST) Special Publication 800-68 and the SANS Institute Password Protection Policy. The Contractor shall:

1) Implement the following security controls on each server, workstation, or portable (e.g., laptop computer) computing device that processes or stores confidential, personal, or sensitive data:

a) Network-based firewall and/or personal firewall

b) Continuously updated anti-virus software

c) Patch-management process including installation of all operating system/software vendor security patches

- 2) Encrypt all confidential, personal, or sensitive data stored on portable electronic media (including, but not limited to, CDs and thumb drives) and on computing devices (including, but not limited to, desktop computers, laptop computers and PDAs) with a solution that uses proven industry standard algorithms.
- 3) Prior to disposal, sanitize all DMH confidential data contained in hard drives, memory devices, portable electronic storage devices, mobile computing devices, and networking equipment in a manner consistent with the National Institute of Standards and Technology (NIST) Special Publication 800-88.

The Contractor shall not transmit confidential, personal, or sensitive data via e-mail or other Internet transport protocol over a public network unless, at minimum, a 128-bit encryption method (for example AES, 3DES, or RC4) is used to secure the data.

- E. **Mitigation of Harmful Effects.** Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PHI by Contractor or its subcontractors in violation of the requirements of this Agreement.
- F. **Reporting of Improper Disclosures.** Contractor shall report to DMH within twenty-four (24) hours during a work week, of discovery by Contractor that PHI has been used or disclosed other than as provided for by this Agreement.
- G. **Agents and Subcontractors of the Contractor.** Contractor shall ensure that any agent, including a subcontractor to which the Contractor provides PHI received from, or created or received by the Contractor on behalf of DMH, shall comply with the same restrictions and conditions that apply through this Agreement to the Contractor with respect to such information.
- H. **Internal Practices.** Contractor shall make Contractor's internal practices, books and records relating to the use and disclosure of PHI received from DMH, or created or received by the Contractor on behalf of DMH, available to DMH or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by DMH or by the Secretary, for purposes of determining DMH's compliance with the HIPM regulations.
- I. **Notification of Electronic Breach or Improper Disclosure.** During the term of this Agreement, Contractor shall notify DMH immediately upon discovery of any breach of Medi-Cal IHI and/or data, where the information and/or data is reasonably believed to have been acquired by an unauthorized person. Immediate notification shall be made to the DMH Information Security Officer, within two business days of discovery, at (916) 651-6776. Contractor shall take prompt corrective action to cure any deficiencies and any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations. Contractor shall investigate such breach and provide a written report of the investigation to the DMH Information Security Officer, postmarked within thirty (30) working days of the discovery of the breach to the address below:

**Information Security Officer
Office of HIPAA Compliance
California Department of Mental Health
1600 9th Street, Room 102
Sacramento, CA 95814**

- J. **Employee Training and Discipline:** Contractor shall train and use reasonable measures to ensure compliance with the requirements of this Agreement by employees who assist in the performance of functions or activities on behalf of DMH under this Agreement and use or disclosure of IHI; and discipline such employees who intentionally violate any provisions of this Agreement, including by termination of employment.
- K. **Effect of Termination.** Upon termination or expiration of this Agreement for any reason, Contractor shall return or destroy all IHI received from DMH (or created or received by Contractor on behalf of DMH) that Contractor still maintains in any form, and shall retain no copies of such IHI or, if return or destruction is not feasible, it shall continue to extend the protections of this Agreement to such information, and limit further use of such IHI to those purposes that make the return or destruction of such IHI infeasible. This provision shall apply to IHI that is in the possession of subcontractors or agents of the Contractor.
- L. **Miscellaneous Provisions.**
 - 1) **Disclaimer.** DMH makes no warranty or representation that compliance by Contractor with this Agreement, HIPAA or the HIPAA regulations shall be adequate or satisfactory for Contractor's own purposes or that any information in the Contractor's possession or control, or transmitted or received by the Contractor, is or shall be secure from unauthorized use or disclosure. Contractor is solely responsible for all decisions made by Contractor regarding the safeguarding of IHI.

- 2) Assistance in Litigation or Administrative Proceedings. Contractor shall make itself, and use its best efforts to make any subcontractors, employees or agents assisting Contractor in the performance of its obligations under this Agreement, available to DMH at no cost to DMH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DMH, its directors, officers or employees for claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy based upon actions or inactions of the Contractor and/or its subcontractor, employee, or agent, except where Contractor or its subcontractor, employee, or agent is a named adverse party.
 - a) No Third-Party Beneficiaries. Nothing expressed or implied in the terms and conditions of this Agreement is intended to confer, nor shall anything herein confer, upon any person other than DMH or Contractor and their respective successors or assignees, any rights remedies, obligations or liabilities whatsoever.
 - b) Interpretation. The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HIPAA regulations and applicable State laws. The parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA regulations.
 - c) Regulatory References. A reference in the terms and conditions of this Agreement to a section in the HIPAA regulations means the section as in effect or as amended.
 - d) Survival. The respective rights and obligations of Contractor under Section 6.C of this Agreement shall survive the termination or expiration of this Agreement.
- 3) Violations reported to U.S. Department of Health and Human Services. Upon DMH's knowledge of a material breach of this Agreement by Contractor, that has not been cured or for which termination of the Agreement is not feasible, the DMH Information Security Officer shall report the violation to the Secretary of the U.S. Department of Health and Human Services.
- 4) Judicial or Administrative Proceedings. DMH may terminate this Agreement, effective immediately, if (i) Contractor is found guilty in a civil or criminal proceeding for a violation of the HIPAA Privacy or Security Rule or (ii) a finding or stipulation that the Contractor has violated a privacy or security standard or requirement of HIPAA, or other security or privacy laws is made in an administrative or civil proceeding in which the Contractor is a party.

Agreement 354-158-M-E2009, Exhibit E HIPAA Business Associate Agreement

This Business Associate Agreement is made part of the base contract ("Underlying Agreement") to which it is attached, as of the date of commencement of the term of the Underlying Agreement (the "Effective Date").

RECITALS

WHEREAS, COUNTY and CONTRACTOR (hereinafter referred to as Business Associate ("BA")) entered into the Underlying Agreement pursuant to which BA provides services to COUNTY, and in conjunction with the provision of such services, certain Protected Health Information ("PHI") and Electronic Protected Health Information ("EPHI") may be disclosed to BA for the purposes of carrying out its obligations under the Underlying Agreement; and

WHEREAS, the COUNTY and BA intend to protect the privacy and provide for the security of PHI and EPHI disclosed to BA pursuant to the Agreement in compliance with the Health Insurance Portability and Accountability Act, Pub. L. No. 104-191 of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the "HITECH" Act), and regulation promulgated thereunder by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws as may be amended from time to time; and

WHEREAS, COUNTY is a Covered Entity, as defined in the Privacy Rule and Security Rule, including but not limited to 45 CFR Section 160.103; and

WHEREAS, BA, when a recipient of PHI from COUNTY, is a Business Associate as defined in the Privacy Rule, the Security Rule, and the HITECH Act, including but not limited to 42 USC Section 17938 and 45 CFR Section 160.103; and

WHEREAS, "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.202(g);

WHEREAS, "Breach" shall have the meaning given to such term under the HITECH Act under 42 USC Section 17921; and

WHEREAS, "Unsecured PHI" shall have the meaning to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to 42 USC Section 17932(h).

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the Parties agree as follows:

1. Definitions. Unless otherwise provided in this Business Associate Agreement, capitalized terms shall have the same meanings as set forth in the Privacy Rule, as may be amended from time to time.

2. Scope of Use and Disclosure by BA of County Disclosed PHI
- A. BA shall not disclose PHI except for the purposes of performing BA's obligations under the Underlying Agreement. Further, BA shall not use PHI in any manner that would constitute a violation of the minimum necessary policies and procedures of the COUNTY, Privacy Rule, Security Rule, or the HITECH Act.
- B. Unless otherwise limited herein, in addition to any other uses and/or disclosures permitted or authorized by this Business Associate Agreement or required by law, BA may:
- (1) use the PHI in its possession for its proper management and administration and to fulfill any legal obligations.
 - (2) disclose the PHI in its possession to a third party for the purpose of BA's proper management and administration or to fulfill any legal responsibilities of BA, or as required by law
 - (3) disclose PHI as necessary for BA's operations only if:
 - (a) prior to making a disclosure to a third party, BA will obtain written assurances from such third party including:
 - (i) to hold such PHI in confidence and use or further disclose it only for the purpose of which BA disclosed it to the third party, or as required by law; and,
 - (ii) the third party will immediately notify BA of any breaches of confidentiality of PHI to extent it has obtained knowledge of such breach.
 - (4) aggregate the PHI and/or aggregate the PHI with that of other data for the purpose of providing COUNTY with data analyses related to the Underlying Agreement, or any other purpose, financial or otherwise, as requested by COUNTY.
 - (5) not disclose PHI disclosed to BA by COUNTY not authorized by the Underlying Agreement or this Business Associate Agreement without patient authorization or de-identification of the PHI as authorized in writing by COUNTY.
 - (6) de-identify any and all PHI of COUNTY received by BA under this Business Associate Agreement provided that the de-identification conforms to the requirements of the Privacy Rule, 45 CFR and does not preclude timely payment and/or claims processing and receipt.
- C. BA agrees that it will neither use nor disclose PHI it receives from COUNTY, or from another business associate of COUNTY, except as permitted or required by this Business Associate Agreement, or as required by law, or as otherwise permitted by law.

3. Obligations of BA. In connection with its use of PHI disclosed by COUNTY to BA, BA agrees to:
 - A. Implement appropriate administrative, technical, and physical safeguards as are necessary to prevent use or disclosure of PHI other than as permitted by the Agreement that reasonably and appropriately protects the confidentiality, integrity, and availability of the PHI in accordance with 45 CFR 164.308, 164.310, 164.312, and 164.504(e)(2). BA shall comply with the policies and procedures and documentation requirements of the HIPAA Security Rule.
 - B. Report to COUNTY within 24 hours of any suspected or actual breach of security, intrusion, or unauthorized use or disclosure of PHI of which BA becomes aware and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. BA shall take prompt corrective action to cure any such deficiencies and any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.
 - C. Report to COUNTY in writing of any access, use or disclosure of PHI not permitted by the Underlying Agreement and this Business Associate Agreement, and any Breach of Unsecured PHI of which it becomes aware without unreasonable delay and in no case later than five (5) days. To the extent the Breach is solely a result of BA's failure to implement reasonable and appropriate safeguards as required by law, and not due in whole or part to the acts or omissions of the COUNTY, BA may be required to reimburse the COUNTY for notifications required under 45 CFR 164.404 and CFR 164.406.
 - D. BA shall not use or disclose PHI for fundraising or marketing purposes. BA shall not disclose PHI to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates. BA shall not directly or indirectly receive remuneration in exchange of PHI, except with the prior written consent of the COUNTY and as permitted by the HITECH Act, 42 USC Section 17935(d)(2); however, this prohibition shall not affect payment by COUNTY to BA for services provided pursuant to the Agreement.
4. PHI Access, Amendment and Disclosure Accounting. BA agrees to:
 - A. Provide access, at the request of COUNTY, within five (5) days, to PHI in a Designated Record Set, to the COUNTY, or to an Individual as directed by the COUNTY. If BA maintains an Electronic Health Record, BA shall provide such information in electronic format to enable COUNTY to fulfill its obligations under the HITECH Act, including, but not limited to, 42 USC Section 17935(e).
 - B. Within ten (10) days of receipt of a request from COUNTY, incorporate any amendments or corrections to the PHI in accordance with the Privacy Rule

in the event that the PHI in BA's possession constitutes a Designated Record Set.

- C. To assist the COUNTY in meeting its disclosure accounting under HIPAA:
- (1) BA agrees to implement a process that allows for an accounting to be collected and maintained by BA and its agents or subcontractors for at least six (6) years prior to the request. However, accounting of disclosure from Electronic Health Record for treatment, payment, or health care operations purposes are required to be collected and maintained for only three (3) years prior to the request, and only to the extent that BA maintains an electronic health record and is subject to this requirement. At the minimum, the information collected shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if know, the address of the entity or person; (iii) a brief description of PHI disclosed and; (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure.
 - (2) Within in 30 days of notice by the COUNTY, BA agrees to provide to COUNTY information collected in accordance with this section to permit the COUNTY to respond to a request by an Individual for an accounting of disclosures of PHI.
- D. Make available to the COUNTY, or to the Secretary of Health and Human Services (the "Secretary"), BA's internal practices, books and records relating to the use of and disclosure of PHI for purposes of determining BA's compliance with the Privacy Rule, subject to any applicable legal restrictions. BA shall provide COUNTY a copy of any PHI that BA provides to the Secretary concurrently with providing such information to the Secretary.
5. Obligations of COUNTY.
- A. COUNTY agrees that it will promptly notify BA in writing of any restrictions on the use and disclosure of PHI agreed to by COUNTY that may affect BA's ability to perform its obligations under the Underlying Agreement, or this Business Associate Agreement.
 - B. COUNTY agrees that it will promptly notify BA in writing of any changes in, or revocation of, permission by any Individual to use or disclose PHI, if such changes or revocation may affect BA's ability to perform its obligations under the Underlying Agreement, or this Business Associate Agreement.
 - C. COUNTY agrees that it will promptly notify BA in writing of any known limitation(s) in its notice of privacy practices to the extent that such limitation may affect BA's use of disclosure of PHI.

- D. COUNTY shall not request BA to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by COUNTY, except as may be expressly permitted by the Privacy Rule.
- E. COUNTY will obtain any authorizations necessary for the use or disclosure of PHI, so that BA can perform its obligations under this Business Associate Agreement and/or the Underlying Agreement.

6. Term and Termination.

- A. Term. This Business Associate Agreement shall commence upon the Effective Date and terminate upon the termination of the Underlying Agreement, as provided therein when all PHI provided by the COUNTY to BA, or created or received by BA on behalf of the COUNTY, is destroyed or returned to the COUNTY, or, or if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.
- B. Termination for Cause. Upon the COUNTY's knowledge of a material breach by the BA, the COUNTY shall either:
 - (1) Provide an opportunity for the BA to cure the breach or end the violation and terminate this Agreement if the BA does not cure the breach or end the violation within the time specified by the COUNTY.
 - (2) Immediately terminate this Agreement if the BA has breached a material term of this Agreement and cure is not possible; or
 - (3) If neither termination nor cures are feasible, the COUNTY shall report the violation to the Secretary.
- C. Effect of Termination.
 - (1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, the BA shall, at the option of COUNTY, return or destroy all PHI that BA or its agents or subcontractors still maintain in any form, and shall retain no copies of such PHI.
 - (2) In the event that the COUNTY determines that returning or destroying the PHI is infeasible, BA shall provide to the COUNTY notification of the conditions that make return or destruction infeasible, and . BA shall extend the protections of this Agreement to such PHI to those purposes that make the return or destruction infeasible, for so long as the BA maintains such PHI. If COUNTY elects destruction of the PHI, BA shall certify in writing to COUNTY that such PHI has been destroyed.

7. Indemnity

- A. BA shall indemnify and hold harmless all Agencies, Districts, Special Districts and Departments of the COUNTY, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives (collectively "COUNTY") from any liability whatsoever, based or asserted upon any services of BA, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to BA's performance under this Business Associate Agreement, including but not limited to property damage, bodily injury, or death or any other element of any kind or nature whatsoever including fines, penalties or any other costs and resulting from any reason whatsoever to the extent arising from the performance of BA, its officers, agents, employees, subcontractors, agents or representatives under this Business Associate Agreement. BA shall defend, at its sole expense, all costs and fees including but not limited to attorney fees, cost of investigation, defense and settlements or awards against the COUNTY in any claim or action based upon such alleged acts or omissions.
- B. With respect to any action or claim subject to indemnification herein by BA, BA shall, at its sole cost, have the right to use counsel of its choice, subject to the approval of COUNTY, which shall not be unreasonably withheld, and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of COUNTY; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes BA's indemnification of COUNTY as set forth herein. BA's obligation to defend, indemnify and hold harmless COUNTY shall be subject to COUNTY having given BA written notice within a reasonable period of time of the claim or of the commencement of the related action, as the case may be, and information and reasonable assistance, at BA's expense, for the defense or settlement thereof. BA's obligation hereunder shall be satisfied when BA has provided to COUNTY the appropriate form of dismissal relieving COUNTY from any liability for the action or claim involved.
- C. The specified insurance limits required in the Underlying Agreement of this Business Associate Agreement shall in no way limit or circumscribe BA's obligations to indemnify and hold harmless the COUNTY herein from third party claims arising from the issues of this Business Associate Agreement.
- D. In the event there is conflict between this clause and California Civil Code Section 2782, this clause shall be interpreted to comply with Civil Code Section 2782. Such interpretation shall not relieve the BA from indemnifying the COUNTY to the fullest extent allowed by law.
- E. In the event there is a conflict between this indemnification clause and an indemnification clause contained in the Underlying Agreement of this Business Associate Agreement, this indemnification shall only apply to the subject issues included within this Business Associate Agreement.

8. Amendment The parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for COUNTY to comply with the Privacy Rule, 45 CFR, and HIPAA generally.
9. Survival The respective rights and obligations of this Business Associate Agreement shall survive the termination or expiration of this Business Associate Agreement.
10. Regulatory References A reference in this Business Associate Agreement to a section in the Privacy Rule means the section as in effect or as amended.
11. Conflicts Any ambiguity in this Business Associate Agreement and the Underlying Agreement shall be resolved to permit COUNTY to comply with the Privacy Rule, 45 CFR, and HIPAA generally.