AGREEMENT FOR SERVICES #293-162-M-E2011
Amador County Psychiatrist Services

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 EDC) and Amador County, also a political subdivision of the State of California, whose principal place of business is 810 Court Street, Jackson, CA 95642 (hereinafter referred to as AMADOR);

RECITALS

WHEREAS, EDC has determined that it is necessary to obtain a contractor to provide adult outpatient psychiatric services for the EDC Health Services Department, Mental Health Division (MHD) on a mutually-agreed upon schedule; and

WHEREAS, AMADOR has represented to EDC that it has staff who are specially trained, experienced, expert and competent to perform the special services required hereunder and EDC 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, EDC has determined that the provision of these services provided by AMADOR 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 County of El Dorado Charter, Section 210 (b) (6) and/or Government Code 31000;

NOW, THEREFORE, EDC and AMADOR mutually agree as follows:

Article I. SCOPE OF SERVICES

Section 1.01 EDC Director of Health Services and AMADOR Director of Health Services will agree in writing on the normal hours, schedule and location of work to be performed. Initial agreed-upon schedule shall have AMADOR psychiatrist on-site at EDC facility each Wednesday for approximately nine (9) hours; any planned changes to the normal hours, schedule and location of work will be mutually agreed upon. AMADOR psychiatrist staff will notify EDC's Mental Health Medical Director, giving as much advance notice as possible, of any planned or unanticipated periods during which AMADOR staff will be unavailable.

Section 1.02 AMADOR agrees to furnish psychiatrist staff to provide mental health psychiatric services to clients of EDC as requested in writing by EDC. Services shall include, but may not be limited to:

(a) Providing direct outpatient psychiatric medical care to adults in various EDC facilities and locations, and by use of EDC videoconferencing / telemedicine systems to perform services at remote EDC locations when appropriate and requested by EDC.

(b) Evaluating patients to determine therapeutic and psychiatric / medical needs, including EDC conservatees for purposes of Lanterman-Petris-Short (LPS) renewals.

(c) Administering and interpreting various psychological assessment instruments.

(d) Developing treatment plans; participating in case conferences and consulting with clinical staff regarding support services and treatment options.

(e) Developing, following up and instructing others in appropriate psychiatric / medical protocols.

(f) Prescribing and administering medication to patients as necessary.

(g) Performing crisis intervention as required; assisting clinical staff in mitigating crisis situations; prescribing and administering medication to patients in crisis situations, if deemed necessary.

(h) Evaluating patients for voluntary and involuntary commitment; signing required commitment forms for clients requiring psychiatric hospitalization based upon patient symptoms.

(i) Performing detailed patient record documentation by day's end using the InterTrac system, or subsequent replacement system, and in compliance with both MHD and regulatory standards and requirements; preparing intake and discharge summaries, progress notes and treatment reviews.

(j) Completing and submitting an EDC timecard documenting all days and hours worked, a sample of which is attached hereto as Exhibit A, and incorporated by reference herein.

(k) Participating in relevant investigations, utilization review, quality assurance, quality improvement and program evaluation measures, as directed by EDC Mental Health Medical Director.

(l) Participating in mandatory and relevant training, as directed by EDC Mental Health Medical Director.

(m) Meeting with EDC Counsel in preparation for court proceedings, arbitrations, depositions or administrative hearings related to work performed by AMADOR staff under this Agreement.

(n) Attending and providing testimony at any court proceedings, arbitration, depositions, or administrative proceedings relating to work performed by AMADOR staff under this Agreement.

Section 1.03 AMADOR psychiatric staff providing services under this Agreement shall be requested to review and comply with the "El Dorado County Computer and Network Resource Usage Policies and Standards Guide," attached hereto as Exhibit B, or any update or revision as may be approved by the EDC Board of Supervisors. Furthermore, AMADOR staff providing services under this Agreement shall sign the "County User Agreement" contained on page 12 of Exhibit B.

Section 1.04 EDC agrees to provide the following:

(a) Scheduling of clients.

(b) Office location for AMADOR staff to work in and see clients.

(c) Standard office equipment including access to a computer.

(d) Transcription assistance for psychiatric assessments, as needed,

(e) A copy of each timecard submitted pursuant to Section 1.02 (j) to AMADOR Health Services Department on a monthly basis.

Article II. TERM

This Agreement shall become effective upon final execution by both parties hereto and shall continue for twelve (12) months unless earlier terminated pursuant to the provisions under Article IX herein.

Article III. COMPENSATION FOR SERVICES

AMADOR shall submit monthly invoices detailing days and hours worked, no later than thirty (30) days following the end of a "service month" except in those instances where AMADOR obtains written approval from EDC Health Services Department 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 AMADOR provides services in accordance with Article I - Scope of Services.

For services provided herein, EDC agrees to review, and approve or question invoices within fifteen (15) days of receipt. EDC agrees to pay AMADOR monthly in arrears and within forty-five (45) days following approval of itemized invoice(s) identifying services rendered.

Section 3.01 Rates: $150 / hour

Section 3.02 Not-to-Exceed: $70,000 over the term of this Agreement.

Section 3.03 Invoices shall be submitted to:

Health Services Department – Finance Unit
929 Spring Street
Placerville, CA 95667

Article IV. LICENSE AND CLEARANCE REQUREMENTS

Section 4.01 AMADOR has provided evidence of and shall ensure psychiatrist staff providing services under this Agreement maintains the following:

- Valid California Driver's license.
- Valid Physician and Surgeon Certificate issued by the State of California Board of Medical Examiners.
- Certification by the American Board of Psychiatry as a psychiatrist, or proof of eligibility for certification.
- Medical license number.
- Social Security Number.

Section 4.02 Various EDC facilities maintain their own security requirements. AMADOR will ensure psychiatrist staff cooperates with providing all Live Scan and / or fingerprinting as required by any EDC facility where services will be performed.

Article V. SPECIAL TERMS AND CONDITIONS

By signing this Agreement, AMADOR acknowledges that its employees, while acting in the course and scope of their duties under this Agreement, are subject to all terms and conditions of this Agreement, including but not limited to:

Section 5.01 HIPAA Compliance: By signing this Agreement, AMADOR agrees to adhere to Exhibit C, Business Associate Agreement, attached hereto and incorporated by reference herein.

Section 5.02 Mandated Reporter Requirements: By signing this Agreement, AMADOR acknowledges that its employees are subject to mandated reporter requirements, including but not limited to:

(a) Mandated reporter requirements pursuant to the provisions of Welfare and Institutions Code 15630 related to elder and dependent adults.

(b) 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.

Section 5.03 Debarment & Suspension: By signing this Agreement, AMADOR acknowledges that its employees, while acting in the course and scope of their duties under this Agreement, are subject to applicable Federal suspension and debarment regulations including, but not limited to Title 45 Code of Federal Regulations (CFR) 76.

(a) By signing this Agreement, AMADOR certifies to the best of its knowledge and belief, that it and its principals:

(i) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal department or agency;

(ii) Have not within a three (3) 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;

(iii) 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 herein;

(iv) 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;

(v) Shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under Federal regulations (i.e., 48 CFR part 9, subpart 9.400), debarred, suspended, declared ineligible or voluntarily excluded from participation in such transactions, unless authorized by the State; and

(vi) 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.

(b) The terms and definitions herein have the meanings set out in the Definitions and Coverage sections of the rules implementing Federal Executive Order 12549 (1986) as amended by Federal Executive Order 12689 (1989).

(c) If AMADOR knowingly violates this certification, in addition to other remedies available to the Federal Government, EDC may terminate this agreement for cause or default.

Article VI. 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 VII. AMADOR TO EDC

It is understood that the services provided under this Agreement shall be prepared in and with cooperation from EDC and its staff. It is further agreed that in all matters pertaining to this Agreement, AMADOR shall act as Contractor only to EDC 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 AMADOR's responsibilities to EDC during term hereof.

Article VIII. ASSIGNMENT AND DELEGATION

AMADOR is engaged by EDC for its unique qualifications and skills as well as those of its personnel. AMADOR 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 EDC. In the event EDC agrees in writing that AMADOR may subcontract for services under this Agreement, AMADOR shall require that all subcontractors comply with all terms and conditions of this Agreement, and all pertinent Federal and State statutes and regulations.

Article IX. INDEPENDENT CONTRACTOR/LIABILITY

Section 9.01 AMADOR 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. AMADOR 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.

Section 9.02 AMADOR 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. EDC 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 AMADOR or its employees.

Article X. FISCAL CONSIDERATIONS

The parties to this Agreement recognize and acknowledge that EDC is a political subdivision of the State of California. As such, 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 EDC business, EDC 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.

Notwithstanding any other provision of this Agreement to the contrary, EDC 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 EDC released from any further liability hereunder.

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 EDC department for which services were contracted to be performed, pursuant to this paragraph in the sole discretion of EDC, this Agreement may be deemed to be canceled in its entirety subject to payment for services performed prior to cancellation.

Article XI. DEFAULT, TERMINATION, AND CANCELLATION

Section 11.01 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.

Section 11.02 Bankruptcy
This Agreement, at the option of the EDC, shall be terminable in the case of bankruptcy, voluntary or involuntary, or insolvency of AMADOR.

Section 11.03 Ceasing Performance
EDC may terminate this Agreement in the event AMADOR ceases to operate as a business, or otherwise becomes unable to substantially perform any term or condition of this Agreement.

Section 11.04 Termination or Cancellation without Cause
EDC may terminate this Agreement in whole or in part upon seven (7) calendar days written notice by EDC without cause. If such prior termination is effected, EDC will pay for satisfactory services rendered prior to the effective dates as set forth in the Notice of Termination provided to AMADOR, and for such other services, which EDC may agree to in writing as necessary for contract resolution. In no event, however, shall EDC be obligated to pay more than the total amount of the contract. Upon receipt of a Notice of Termination, AMADOR 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 XII. 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 EDC 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 AMADOR shall be addressed as follows:

AMADOR COUNTY – HEALTH & HUMAN SERVICES
10877 CONDUCTOR BLVD, SUITE 300
SUTTER CREEK, CA 95685-9682
ATTN: KRISTIN BENGYEL, HEALTH SERVICES DIRECTOR

or to such other location as the AMADOR directs.

Article XIII. INDEMNITY

AMADOR shall indemnify, defend and hold harmless EDC, its officers, agents, employees and representatives from and against any and all claims, losses, liabilities or damages, demands and actions including payment of reasonable attorney's fees, arising out of or resulting from the performance of this Agreement, caused in whole or in part by any negligent or willful act or omission of AMADOR, its officers, agents, employees, subcontractors, or anyone directly or indirectly employed by any of them regardless of whether caused in part by a party indemnified hereunder.

EDC shall indemnify, defend and hold harmless AMADOR, its officers, agents, employees and representatives from and against any and all claims, losses, liabilities or damages, demands and actions including payment of reasonable attorney's fees, arising out of or resulting from the performance of this Agreement, caused in whole or in part by any negligent or willful act or omission of EDC, its officers, agents, employees, subcontractors, or anyone directly or indirectly employed by any of them regardless of whether caused in part by a party indemnified hereunder.

Article XIV. INSURANCE

Section 14.01 AMADOR shall provide proof of a policy of insurance satisfactory to the County of El Dorado Risk Manager and documentation evidencing that AMADOR maintains insurance that meets the following requirements:

(a) Full Workers' Compensation and Employers' Liability Insurance covering all employees of AMADOR as required by law in the State of California; and
(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 AMADOR in the performance of the Agreement.

Section 14.02 In the event AMADOR 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 14.03 AMADOR 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 14.04 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 14.05 AMADOR 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, AMADOR 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 AMADOR agrees that no work or services shall be performed prior to the giving of such approval. In the event the AMADOR 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.

Section 14.06 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 14.07 The AMADOR's insurance coverage shall be primary insurance as respects the COUNTY, its officers, officials, employees and volunteers. Any insurance or self-insurance maintained by EDC, its officers, officials, employees or volunteers shall be excess of the AMADOR's insurance and shall not contribute with it.

Section 14.08 Any failure to comply with the reporting provisions of the policies shall not affect coverage provided to EDC, its officers, officials, employees or volunteers.

Section 14.09 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 14.10 AMADOR's obligations shall not be limited by the foregoing insurance requirements and shall survive expiration of this Agreement.

Section 14.11 In the event AMADOR cannot provide an occurrence policy, AMADOR 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 14.12 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 EDC.

Article XV. INTEREST OF PUBLIC OFFICIAL

No official or employee of EDC who exercises any functions or responsibilities in review or approval of services to be provided by AMADOR 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 EDC have any interest, direct or indirect, in this Agreement or the proceeds thereof.

Article XVI. INTEREST OF CONTRACTOR

AMADOR covenants that AMADOR 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. AMADOR further covenants that in the performance of this Agreement no person having any such interest shall be employed by AMADOR.

Article XVII. 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. AMADOR attests that it has no current business or financial relationship with any EDC 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. EDC represents that it is unaware of any financial or economic interest of any public officer or employee of AMADOR 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 XVIII. 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 XIX. ADMINISTRATOR

The County Officer or employee with responsibility for administering this Agreement is Christine Kondo-Lister, Deputy Director of Mental Health, or successor.

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

Article XXIII. 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 EDC DEPARTMENT HEAD CONCURRENCE:

By: Neda West
Neda West, Director
Health Services Department

Dated: 4-11-11

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

--COUNTY OF EL DORADO--

By: _____ Dated: _____

Raymond J. Nutting, Chair
Board of Supervisors
COUNTY

Attest: Suzanne Allen de Sanchez
Clerk of the Board of Supervisors

_____ _____
Deputy Date

--AMADOR COUNTY--

By: _____ Dated: _____

John Plasse, Chairman
Board of Supervisors
AMADOR

Attest: Jennifer Burns
Clerk of the Board of Supervisors

_____ _____
Deputy Date

EXHIBIT A

Name Address Address Line #2

INVOICE FOR THE MONTH OF: _____ 2011

WEEK 1	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	TOTAL
DATE						
RATE	$ 150.00	$ 150.00	$ 150.00	$ 150.00	$ 150.00	150.00
HOURS WORKED						0.0
AMOUNT BILLED	0.00	0.00	0.00	0.00	0.00	0.00

WEEK 2	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	TOTAL
DATE						
RATE	$ 150.00	$ 150.00	$ 150.00	$ 150.00	$ 150.00	150.00
HOURS WORKED						0.0
AMOUNT BILLED	0.00	0.00	0.00	0.00	0.00	0.00

WEEK 3	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	TOTAL
DATE						
RATE	$ 150.00	$ 150.00	$ 150.00	$ 150.00	$ 150.00	150.00
HOURS WORKED						0.0
AMOUNT BILLED	0.00	0.00	0.00	0.00	0.00	0.00

WEEK 4	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	TOTAL
DATE						
RATE	$ 150.00	$ 150.00	$ 150.00	$ 150.00	$ 150.00	150.00
HOURS WORKED						0.0
AMOUNT BILLED	0.00	0.00	0.00	0.00	0.00	0.00

WEEK 5	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	TOTAL
DATE						
RATE	$ 150.00	$ 150.00	$ 150.00	$ 150.00	$ 150.00	150.00
HOURS WORKED						0.0
AMOUNT BILLED	0.00	0.00	0.00	0.00	0.00	0.00

MONTHLY TOTAL	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	TOTAL
RATE	$ 150.00	$ 150.00	$ 150.00	$ 150.00	$ 150.00	150.00
HOURS WORKED	0.0	0.0	0.0	0.0	0.0	0.0
AMOUNT BILLED	0.00	0.00	0.00	0.00	0.00	0.00

My signature certifies that the above hours were worked in performance of the agreed upon terms of the contract between El Dorado County Mental Health Department and myself.

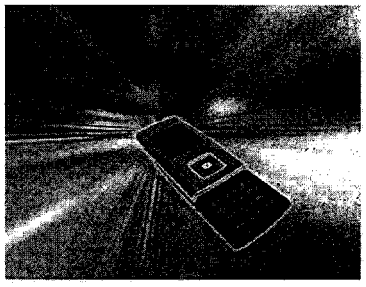
_____

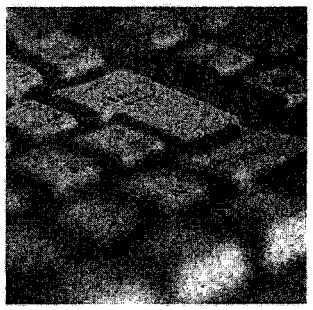
Signature (Date)

El Dorado County

Computer and Network Resource Usage Policies and Standards Guide

General Use

Approved by the Board of Supervisors August 18, 2009

V:\CNUG\CNUG General Approved by BOS 2009-08-18.doc

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

This policy and standards document is subject to periodic revision.

GENERAL USAGE POLICIES

1.1 Background

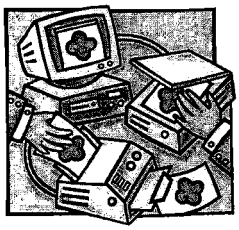
El Dorado County has an extensive communication infrastructure with network and computing resources for use by County employees, contractors, vendors, quasi-governmental employees (fire departments, community services districts, etc.) and temporary workers, hereafter referred to as "County User". In 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.



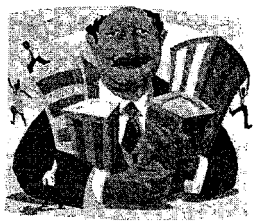
1.2 Purpose

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.

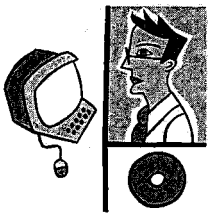
It is the responsibility of the County User to safeguard confidential information from unauthorized disclosure or use. County Users shall not seek to use personal or confidential information for their own use or personal gain. County Users must take all reasonable precautions to ensure privacy is maintained 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.

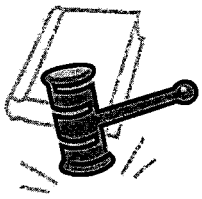
For security and network maintenance purposes, I.T. staff members may monitor equipment, systems and network traffic at any time. This monitoring shall be done under the auspices of this policy, which is incorporated into Board Policy A-19.



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.

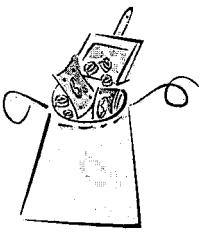
1.5 Compliance with Software Copyright Laws



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.

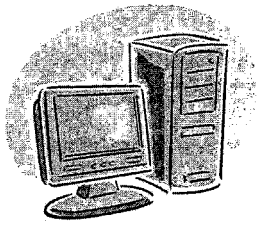
County Users may not make unauthorized copies of copyrighted material including, but not limited to, photographs from magazines, books or other copyrighted sources, copyrighted music, or any copyrighted software for which the County or the County User does not have a valid license.



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 or inaccessible 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.el-dorado.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

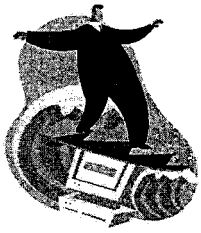
County Users are not responsible for "electronic communication in their possession" when they have no "reasonable" knowledge of its existence or contents.

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

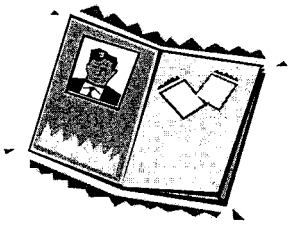
passed and that electronic communication pertaining to litigants no longer needs to be preserved. Preservation may include any and all electronic communication relating to possible litigation being copied onto readable media and delivered (with signed receipt) to County Counsel for later use. By not 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.

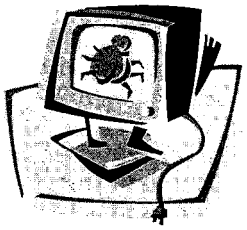
User accounts (e.g., root, enable, NT admin, application administration accounts, etc.) that have system-level privileges or administrative privileges must have strong unique passwords (8-12 character minimum) and will face regular mandatory password changes of no more than every four (4) months.

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.

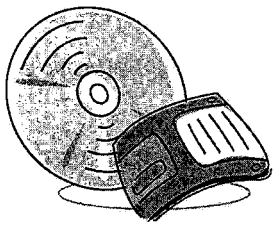
County Users should be cautious of opening electronic communication. Viruses can also be received from persons known to the recipient. If there is any doubt as to the validity of an attachment or the electronic communication, County Users shall delete the electronic communication and/or the attachment.

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.



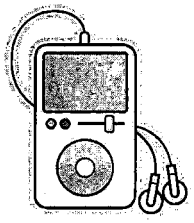
1.12 Removable Data Storage Devices

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.

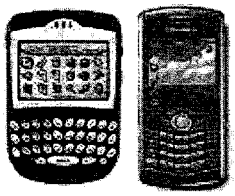
- County digital cameras connected to County computers via docking stations pose little risk and are authorized. Personal digital cameras used in the conduct of County business are authorized to upload digital images.



- 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 us 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.

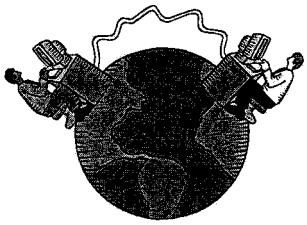
- All portable computer devices must have appropriate County antivirus software installed and County approved firewall software for devices connecting to Internet services to protect data from hackers.

- 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: _____

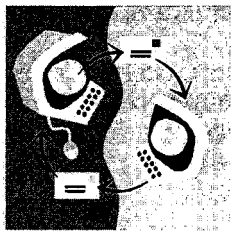
Signature: _____

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.

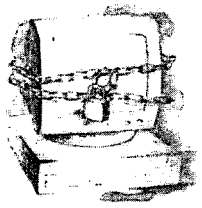
3.1.6 Electronic Communications – Instant Messaging

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:

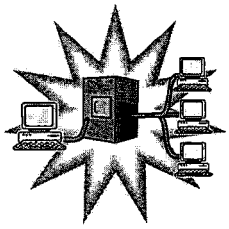
"TheTrafficOn50WasTerribleThisMorning"

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 <u>not recommended.</u>***

- 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 de-compress 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.

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.