COUNTY OF EL DORADO, CALIFORNIA
BOARD OF SUPERVISORS POLICY

Subject:	Policy Number:	Page Number:
PRIVACY AND PROTECTED INFORMATION POLICY	L-1	1 of 80
	Originally Adopted: 08/29/2017	Last Revised Date: 03/21/2023

PURPOSE

A. The purpose of this Privacy and Protected Information Policy is to outline the manner in which the County of El Dorado (County) meets the requirements of both federal and state privacy and confidentiality laws including:
   - 45 Code of Federal Regulations (CFR), Parts 160 and 164, the Health Insurance Portability and Accountability Act of 1996 (HIPAA);
   - Title XIII of Division A of the American Recovery and Reinvestment Act of 2009 (ARRA), called the Health Information Technology for Economic and Clinical Health Act (HITECH);
   - the California Confidentiality of Medical Information Act (CMIA), protecting general physical health information;
   - the Lanterman Petris Short Act (LPS), protecting mental health information;
   - California Health and Safety Code, providing privacy for HIV test results;
   - Patient Access to Health Records Act (PAHRA) providing certain rights to access records maintained by California healthcare providers; and
   - 42 CFR Part 2, protecting certain substance use disorder treatment program records.

   Additional laws and regulations pertaining to privacy matters may also be referred to or cited throughout the policy.

B. The Privacy and Protected Information Policy of the County of El Dorado provides general guidelines and expectations for the necessary collection, creation, use, and disclosure of protected health information about individuals in order to provide services and benefits to individuals, while maintaining reasonable safeguards to protect the privacy of their protected health information. These policies are applicable to all units, divisions, programs or departments within the County of El Dorado that administer and provide health care services.

C. For the purpose of the policy, the terms “confidential information,” “health confidential information,” individual health confidential information,” “protected health confidential information,” “protected health information,” “PHI,” “electronic protected health information,” and “ePHI” will generally be referred to as “PHI.” The meanings and application of these terms include but are not limited to: a subset of health information, including demographic information collected from an individual, and created, received, maintained, or transmitted by a health care provider, health plan, health care clearinghouse, or business associate, that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual,

the past, present, or future payment for the provision of health care to an individual, and identifies the individual, or the confidential information, or creates a reasonable basis to believe it can be used to identify the person; and, includes confidential information in any form, that is transmitted by electronic media, maintained in electronic or other media, or transmitted or maintained in any other form or medium, including the knowledge that an individual receives services or is covered by a County provider or plan.

D. The County of El Dorado and its employees, workforce members, agents, contractors and business associates may collect, maintain, use, transmit, share and/or disclose confidential health information about individuals to the extent needed to administer the County programs, services and activities. County employees, workforce members, agents, contractors and business associates will safeguard all confidential information about individuals and will respect individual privacy rights in accordance with the law and this policy.

E. The policy identifies individuals whose information will be addressed by this policy or who will be subject to this policy as including, but not limited to the following:
    1. clients of County services;
    2. health care providers and county health plan administrators;
    3. Individuals in County detention receiving health care services in correctional settings;
    4. minors and adults receiving mental health, substance use disorder, preventive health and public health services from the County of El Dorado; and,
    5. persons who apply for or are admitted to a county operated or county funded mental health center.

F. For purposes of this policy, confidential health information does not include employment records or education records. Privacy principles for education records are governed by the Family Educational Rights and Privacy Act (FERPA).

G. County staff should always follow the most "stringent" law when it comes to protecting privacy or providing rights to individuals; in some cases, this will mean following California law or other federal laws that provide greater protections than HIPAA, as outlined in the policy. Questions as to which laws take precedent should be directed to the County Department/Agency identified privacy contact or program specific manager/supervisor with consultation to the County Privacy Officer as appropriate.

Subject:	Policy Number:	Page Number:
PRIVACY AND PROTECTED INFORMATION POLICY	L-1	3 of 80
	Originally Adopted: 08/29/2017	Last Revised Date: 03/21/2023

APPROACH

A. Specific policies, protocols, guidelines and procedures within this Privacy and Protected Information Policy are arranged to address the various aspects of individual health care privacy in the County as follows:

1. Part 1 - Administration
   - Purpose
   - Policy - Hybrid Status and Covered Components
   - Personnel - HIPAA Privacy Officer
   - Personnel - HIPAA Security Officer
   - Training/Confidentiality Statement
   - HIPAA Compliance Committee
   - Business Associates and Business Associate Agreements
   - Records Retention
   - Patient Complaint Process

2. Part 2 - Privacy Rule
   - Definitions
   - Minimum Necessary
   - Preemption of More Stringent State/Federal Law
   - De-identified Protected Health Information and Limited Data Sets
   - Mandated Uses and Disclosures
   - Permitted Uses and Disclosures

3. Part 3 - Security Rule
   - Risk Assessment/Analysis
   - Administrative Safeguards
   - Physical Safeguards
   - Technical Safeguards

4. Part 4 - Patients' Rights
   - Notice of Privacy Practices
   - Request for Special Privacy
   - Request for Alternative Communication
   - Access to the Chart
   - Amendment of Records

- Addendum to Records,
- Accounting of Disclosures

5. Part 5 - Breach Reporting Process
   - Breach Incident Reporting (Internal)
   - Investigation
   - Mitigation
   - Sanctions
   - Notification of Patient
   - Reporting to DHHS and State

B. Specific appendices and forms will be made part of the County Privacy and Protected Information Policy and although they may be referred to in an individual Part, copies of forms and samples will all be located and identified in the Appendices. Appendices and forms will be updated from time to time, and will include:

1. HIPAA Complaint Form
2. Request for Access To/Copy of the Record
3. Authorization to Use and Disclose PHI
4. Request for Correction/Addendum to Record
5. Request for Accounting of Disclosures
6. Request for Special Privacy Measures
7. Request for Alternative Communication
8. Sample Letter to Patient Re: Breach
9. Business Associate Agreement Template
10. Notice of Privacy Practices

Policy

For ease of reference, the Privacy and Protected Information Policy is presented in the following sections:

1.0 Administration
- 1.1 Purpose
- 1.2 Policy
- 1.3 References

2.0 Privacy Rule- Uses and Disclosures of PHI
- 2.1 Purpose
- 2.2 Policy

1.0 Administration

1.1 PURPOSE

H. These policies and procedures are intended to ensure compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related state and federal statutes, regulations and contractual obligations governing the privacy, confidentiality and security of protected health information (PHI) and electronic protected health information (ePHI) that is created, maintained, used, accessed and stored by the County of El Dorado (County). This policy addresses the administrative steps that will be taken by the County to establish a comprehensive approach to privacy, confidentiality and security of health information as further described in the policy.

I. Terminology. Any reference in this policy to "PHI" shall include, and be applicable to "ePHI" as well. Any reference in this policy to "patient," "client" or "consumer" shall refer to the recipient of health services, and those terms may be used interchangeably. "Provider" shall refer to the clinician, clinical team or program that treats the patient or provides treatment services to individuals receiving medical or behavioral health care from County clinicians, entities or programs.

J. These policies and procedures apply to all individuals who may access, use, or disclose County PHI in their work on behalf of, or within departments identified as being "covered components" of the "hybrid entity" County, as described in section II-A of this policy.

1.2 POLICY

A. **Hybrid Entity Status/Identification of Covered Components**. The County is a single legal entity that meets the HIPAA definition of a "covered entity" in that it includes in its activities acting as a health care provider that transmits health information in electronic form in connection with HIPAA transactions. However, because some County activities include covered functions, and some County activities include non-covered functions, the governing body has declared that the County is a HIPAA "hybrid entity" with the following "covered components" that are subject to HIPAA:

1. Behavioral Health Services (including, but not limited to Adult & Children's Specialty Mental Health Services, 24-hour Mental Health Crisis Services, Mental Health Services Act (MHSA) Programs, Psychiatric Health Facility, and Substance Use Disorder Services)
2. Public Health Services (including, but not limited to Maternal, Child & Adolescent Health Programs, California Children's Services, Clinical Services, Communicable Disease Control, Immunization and other Public Health Nursing clinical services)
3. Community Services
4. EMS operation and Administration - CAO
5. Probation Department Correctional Healthcare (including physical and behavioral health care services in Juvenile Detention)
6. Sheriff's Department Correctional Healthcare (including physical and behavioral health care services in County Jail)

B. **Personnel - HIPAA Privacy Officer.** The County shall designate a HIPAA privacy official (Privacy Officer) who is responsible for the development and implementation of the policies and procedures governing the privacy and confidentiality of PHI created, maintained, used, accessed and stored by the County.

1. The Privacy Officer, currently Risk Manager shall report through chain of command to HR Director and shall collaborate with the Chief Information Security Officer (HIPAA Security Officer) to assure full compliance with the laws, regulations and contractual obligations the County may have related to the privacy and security of the PHI and ePHI it maintains and stores.
2. The Privacy Officer shall be responsible for bringing complaints related to the County's privacy and confidentiality practices, and any reports of breaches or potential

breaches, to the attention of the HIPAA Compliance Committee, and for implementing all appropriate steps in response to the breach or potential breach as directed by the Committee.

3. The Privacy Officer may delegate responsibilities to others within County Health and Human Services Agency (HHSA), or at individual healthcare facilities or locations, who will oversee the day to day activities of county health and behavioral health services health information management, including the disclosure and release of PHI, supporting consumers in accessing their own PHI, and other related HIPAA rights outlined in County policies and procedures.

C. **Personnel - HIPAA Security Officer. T**he County shall designate a HIPAA security official (Security Officer) who is responsible for assuring that administrative, physical and technical safeguards are in place to protect the security of any PHI and ePHI that is created, maintained, used, accessed and stored by the County.

1. The Security Officer will report to the Information Technologies Department Head and collaborate with the HIPAA Privacy Officer to assure full compliance with the laws, regulations and contractual obligations of the County related to maintaining the security of the PHI and ePHI that County maintains and stores.
2. The Security Officer will be responsible to take all steps necessary to implement, monitor and assure that systems are in place to protect the confidentiality, integrity and availability of the PHI and ePHI created, maintained, used, stored and managed by the County.
3. The Security Officer shall be responsible for performing a risk assessment and analysis, and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by County.
4. The Security Officer shall be responsible for identifying, recommending and implementing security measures sufficient to reduce risk and vulnerabilities to County PHI and ePHI, including developing emergency response plans to any breach or attempted breach, as well as back up plans that will assure the integrity and availability of County PHI and ePHI.

D. **Training/Confidentiality Statement**. The HIPAA Privacy Officer will oversee the training of all members of the County's workforce that provide services to, or within, the County's identified "covered components" that are described in section II-A of this policy. The training shall include a review of the County's HIPAA policies and procedures as necessary and appropriate for the members of the workforce to carry out their functions on behalf of or within the covered components.

1. The Privacy Officer will work with the Security Office and with County Human Resources personnel to assure that workforce orientation includes initial training on the County's efforts to protect the confidentiality, privacy, and security of its PHI and ePHI, and that all staff providing services to, or working within the covered components are trained on a regular basis thereafter.
2. All employees of the County providing services to, or within, the County's "covered components" shall sign the "County of El Dorado Confidentiality Statement" prior to working with any PHI or ePHI, and annually thereafter. Each Department shall be responsible for assuring that these Statements are maintained and current and kept for a minimum of six years after the employment period ends regardless of the reason for the change of status in the employment relationship.
3. Additional training will be provided as deemed appropriate and necessary if there are significant changes in the law, changes in the County's HIPAA policies and procedures, or following a serious potential or actual breach incident.
4. The HIPAA Privacy Officer shall collaborate with County Human Resources staff to ensure that appropriate documentation of all training is maintained for at least six (6) years and that the documentation is readily available should there be a request for that information by a surveyor.

E. **HIPAA Compliance Committee**. The HIPAA Compliance Committee will provide guidance and oversight to individual County departments to assist them with compliance with County HIPAA policies and procedures.
   1. The Compliance Committee will initially be comprised of the following:
      a. Senior Risk Analyst
      b. Risk Manager- HIPAA Compliance Officer/HIPAA Privacy Officer
      c. Chief Information Security Officer/HIPAA Security Officer
      d. HHSA privacy designate (s)
      e. Office of the County Counsel Representative
   2. The HIPAA Compliance Committee will have responsibilities in the following key areas:
      a. Policies and Procedures - The County's HIPAA policies and procedures ("Policies/Procedures") are comprised of both Privacy and Security Policies and Procedures. It is the role of the HIPAA Compliance Committee to create, review, and update the HIPAA policies and procedures as necessary to respond to changes in federal and state law, and to reflect best practices. These policies will be posted on the County of El Dorado Intranet Site.
      b. Breach Investigation/Response - When actual or potential PHI/ePHI breaches or concerns are communicated or reported, the HIPAA Compliance Committee

will be responsible for overseeing the investigation and response. Should a breach be discovered or suspected, the committee will be responsible to follow breach policy/procedures and assure that all required steps are taken, including:

- Correcting processes not working
- Mitigating harm,
- notifying the patient, and
- reporting the breach to the US DHHS.

c. Proposed remedies, solutions and corrective actions will also be the responsibility of the HIPAA Compliance Committee.

3. The HIPAA Compliance Committee will be responsible to conduct or oversee regular internal reviews and audits to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI/ePHI. Reviews shall include site assessments of HIPAA-covered worksites to evaluate the effectiveness of safeguards used in the workplace to protect PHI and ePHI. These assessments will include Privacy and Security policy/procedural requirements for safeguarding PHI and ePHI, incident response and reporting, continuity planning and emergency operations, documentation retention, HIPAA training status, proper retention and destruction of PHI/ePHI, computer workstation safeguards, work area safeguards, user access management, facility security safeguards, Notice of Privacy Practices, client rights, use and disclosure of PHI and ePHI, and medical records. The results of assessments shall be documented, and reports maintained for a minimum of six (6) years. Identified risks will be communicated by the HIPAA Compliance Committee to the appropriate department heads for their attention and follow-up.
4. The HIPAA Compliance Committee will be responsible to create, review and update appropriate HIPAA forms for patient use and for communication of HIPAA-related issues. These forms will include:
   a. Privacy Complaints**:** The Committee is responsible for responding to, investigating and resolving HIPAA-related complaints for internal County of El Dorado programs, whether such complaints are made by consumers or employees. Complaints should be in writing using the County of El Dorado approved “HIPAA Complaint Form” but should also be brought to the Committee’s attention even if other means of communication were used, for example, when there is a verbal complaint from a patient about an alleged serious breach.
   b. Request to Access Health Records: The "Request for Access To/Copy of the Record" form should be encouraged to be used by the client to request access

to, or receive a copy of, their own health information. Other forms or means of requesting access that are clear, conspicuous and specific will also be recognized. The County will not impose unreasonable measures on an individual requesting access to their own PHI whether the individual is the patient or the patient representative, nor will the County create barriers to access, or unreasonably delay the individual from obtaining access.

c. Authorization for Use, Access or Release of Health Information to Third Parties: The County approved "Authorization to Use and Disclose PHI" form that is compliant with HIPAA, Part 2 and state law should be used when an individual wants to permit the county to use, access or disclose their PHI or ePHI to third parties. This form should be used for example, when the patient requests that PHI be released to their attorney, probation officer, social services case worker, employer or school. Release of information forms created by other individuals or entities may be recognized on a case-by-case basis so long as they are HIPAA- and state and federal law-compliant, are not compound, are in 14-point font, and include all required elements and statements.

d. Other forms: The HIPAA Compliance Committee shall oversee the development of other forms that support consumers rights, for example the right to correct or addend their record, request an accounting of disclosures, ask for special privacy protections, or request alternative forms of communication.

F. **Business Associates and Business Associate Agreements**

1. HIPAA defines a "business associate" as an individual or organization that is not part of County's workforce but is a vendor, supplier or service provider that acts on behalf of the County performing functions or activities that the County would itself be permitted to do that require the use or disclosure of protected health information. Typically, a business associate provides accounting, actuarial, claims, auditing, management, consulting, administrative, data analysis or aggregation, utilization review, quality assurance, billing, financial services, accreditation, benefit management, practice management, legal, quality review, records destruction, or patient safety activities.

2. The County may permit a business associate to create, receive, maintain, or transmit PHI or ePHI on its behalf only if the County first obtains satisfactory assurances that the business associate will appropriately safeguard the information through a written Business Associate Agreement (BAA). BAA

language that is otherwise addressed and included in the body of an underlying contract may also meet the required criteria and may be accepted on a case-by-case basis if approved by the Office of County Counsel. All contracts should be handled, reviewed and approved through the appropriate contract protocols established by the County.

3. Determination of Business Associate status should be done anytime a covered component, or individual assisting a covered component, considers bringing in an outside vendor, supplier or contractor where the scope of work will necessarily require the use of, or exposure to County PHI or ePHI.
    a. All proposed or renewed business relationships between third-party entities and the County that potentially involve exposure to County PHI or ePHI shall be first reviewed by the County contracting department, or by the individual County agency seeking to enter the contractual arrangement, in order to clarify Business Associate status prior to executing an agreement with the entity.
    b. If the business relationship is determined to be a Business Associate relationship, a Business Associate Agreement (BAA) shall be prepared and included in the contract signed by the Business Partner Entity as provided in subsection 2 above.
    c. The employee responsible for administering the contract and agreement with the Business Associate will secure appropriate signatures and include the BAA with the contract for approval. Upon approval, a copy of the executed BAA will be provided to the HIPAA Compliance Committee.
4. County employees who receive a report or complaint from any source about inappropriate safeguards to PHI or ePHI by Business Associates shall report the matter to a supervisor, manager, or the HIPAA Compliance Committee. The County will take reasonable steps to cure breaches or end violations, and if unsuccessful, shall work with the Office of County Counsel to take steps to terminate the Business Associate's contract with the County and retrieve all PHI or ePHI in the Business Associate's possession.

G. **Records Retention** - All records related to HIPAA policies and procedures, complaints, investigations, responses, and breaches or potential breaches shall be maintained for a minimum of six (6) years. Designated records sets reflecting patient care, commonly referred to as "patient chart" or "medical record" as well as related billing records shall be

retained for longer periods of time in accordance with the Health Information Management Patient Records Retention schedule, and related policies and procedures.

H. **Patient Complaint Process** - Complaints regarding application of County HIPAA privacy and security policies and procedures should be submitted to the HIPAA Compliance Committee using the Complaint Form designed for this purpose. (See Appendix 1, HIPAA Complaint Form.)

1. Consumers or employees may file complaints concerning:
    a. Disagreements with County's privacy policies and procedures.
    b. Suspected violation(s) related to the use, access, disclosure, or disposal of the client's PHI or ePHI.
    c. Denial of access to an individual to their own PHI or ePHI.
    d. Denial of a request for amendments to PHI or ePHI.
2. Complaints should be filed in writing, either on paper or electronically; if a verbal complaint is received from a patient or member of the public, and there is a reason that a written complaint might not be feasible, then that information should be recorded by staff and forwarded by staff to the HIPAA Compliance Committee.
3. Complaints may also be filed with the County HIPAA Compliance Officer or sent to the Risk Manager in accordance with the County's Notice of Privacy Practices.
4. The complaint should describe the acts or omissions believed to be in violation of the law, or policy and procedure, or the cause of a potential or actual breach, and should, when possible, name the person(s) believed to be involved.
5. County will not intimidate, threaten, coerce, discriminate against or take other retaliatory action against any person filing a complaint or inquiring how to file a complaint.
6. County will not require clients to waive their rights to file a complaint as a condition of providing treatment, qualifying for benefits, enrollment in a health plan, or determining eligibility for benefits.
7. Employees shall immediately forward complaints from clients or co-workers to the HIPAA Privacy Officer, or HIPAA Compliance Committee for appropriate handling in coordination with IT polices.

1.3 REFERENCES

45 CFR Parts 160 and 164.

2.0 Privacy Rule – Uses and Disclosures of PHI

2.1 PURPOSE

A. The purpose of this policy is to provide guidance to staff and clear direction on when a use, access or disclosure of protected health information ("PHI") and Medi-Cal personally identifiable information ("PII") concerning County of El Dorado ("County") patients, clients and consumers (also referred to "individuals") is required, and when a use, access or disclosure is permissible. Any reference in the policy to "PHI" shall be deemed to include PII as well. In any cases where County staff is unsure of the rules that might apply, the Department Privacy Officer or supervising program manager. If questions remain, supervisory staff should take the question to the HIPAA Privacy Officer or Compliance Committee as appropriate.

B. This policy also provides guidance to staff on the "minimum necessary" rule, and provides examples of how this rule can be applied to situations where information can be de-identified prior to disclosure.

C. The purpose of this policy is to also clearly explain the "preemption rule" that requires that the most stringent law be followed, so long as there is no conflict with HIPAA, in cases where more than one law governs the privacy of health information, for example where California laws provide rules for protecting the privacy of physical health information (CMIA), mental health information (LPS Act), and HIV information (CA Health and Safety Code), and where federal law, at 42 CFR Part 2, provides more stringent rules concerning the confidentiality of substance use disorder treatment program records.

2.2 POLICY

A. Minimum Necessary Rule (45 CFR 164.502; 45 CFR 164.514)

1. When using or disclosing PHI or requesting it from other covered entities or business associates, County employees shall make reasonable efforts to limit the use, request or disclosure to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
2. This rule shall not apply to:
   a. Disclosures to or requests for information by a health care provider for treatment;
   b. Uses or disclosures made to the individual when permitted or required;
   c. Uses or disclosures made pursuant to written authorization of the individual;
   d. Uses or disclosures to the Secretary of DHHS as required by HIPAA;
   e. Uses or disclosures that are otherwise required by law so long as they are limited to

what the law requires;

f. Uses or disclosures that are required to comply with the HIPAA regulations, including the Privacy Rule and Security Rule.

3. In order to implement the minimum necessary standard and determine when a use, access or disclosure is appropriate, the County shall identify those persons or classes of persons in its workforce who need access to PHI to carry out their duties, and for each person or class of persons identified, describe the category or categories of PHI to which access is needed and any conditions appropriate to such access.
4. The County shall make reasonable efforts to limit the access of such persons or classes of persons identified in subsection (3) above to only that PHI necessary to their duties.
5. For disclosures or requests for PHI that are made on a routine and recurring basis, the County will implement rules and guidelines (which may be standard protocols) that limit the PHI disclosure to the amount reasonably necessary to achieve the purpose of the disclosure; whenever possible information will first be de-identified by removing identifiers when it is used, for example, for internal operations purposes such as peer review.
6. For all other disclosures or its own requests for disclosures the County shall develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought and review the disclosures or its own requests for disclosure on an individual basis in accordance with such criteria.
7. The County may rely, if such reliance is reasonable, on a requested disclosure as the minimum necessary for the stated purpose a) when making disclosures to public officials that are permitted by the Privacy Rule at 45 CFR 164.512, if the official represents that the information requested is the minimum necessary for the stated purpose, b) when requested by another HIPAA covered entity, c) when requested by a professional who is a member of the County's workforce or is a business associate providing professional services to the County if the professional represents that the information requested is the minimum necessary for the stated purpose, or d) when documentation or representations that comply with the requirements related to disclosures for research purposes have been provided by the person requesting the information.
8. The County will limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when making such requests from other covered entities.

B. De-Identification of Information

1. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information, or PHI.

2. The County can determine that health information is not individually identifiable health information only if:
   a. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, applies those principles and methods and determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information, and documents the methods and results of the analysis that justify that determination; or
   b. The following identifiers of the individual or of relatives, employers, or household members of the individual are removed:
      1) Names;

      2) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

      3) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

      4) Telephone numbers;

      5) Fax numbers;

      6) Electronic mail addresses;

      7) Social security numbers;

      8) Medical record numbers;

9) Health plan beneficiary numbers;

10) Account numbers;

11) Certificate/license numbers;

12) Vehicle identifiers and serial numbers, including license plate numbers;

13) Device identifiers and serial numbers;

14) Web Universal Resource Locators (URLs);

15) Internet Protocol (IP) address numbers;

16) Biometric identifiers, including finger and voice prints;

17) Full face photographic images and any comparable images;

18) Any other unique identifying number, characteristic, or code, except for codes or other means of record identification that are not derived or related to information about the individual or otherwise capable of being translated so as to identify the individual, and the code is not disclosed; and

19) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

C. Pre-emption Rule and Concept of "More Stringent Law" (45 CFR Part 160, Subpart B)

1. HIPAA regulations recognize that other laws may also provide privacy protections to confidential health information and provide that the more stringent law should prevail so long as it is not contrary to HIPAA, and so long as it does not interfere with disclosures to the Secretary of DHHS or to the patient seeking access to their own PHI.
2. "More stringent" means that the law that is followed or portion thereof, is the law or portion of the law that prohibits or limits a use or disclosure even though HIPAA regulations would otherwise permit it and provides greater privacy protection for the individual, and in the case of rights of an individual related to access or amendment of the PHI, would permit the greater rights of access to, or amendment of the information, and would apply the rights to the greater amount of information; it also means anything that

would increase the privacy protections afforded the individual or the rights that are enjoyed.

3. "More stringent" in terms of recordkeeping or requirements related to accounting of disclosures means that the law that is followed would provide for retention or reporting of more detailed information or for a longer duration.
4. The general pre-emption rule does not apply to state laws that might be contrary to a HIPAA provision if the state law establishes procedures for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.
5. The County has adopted policies and procedures related to uses and disclosures of PHI and for the administration of its programs, services and activities that recognize HIPAA and the pre-emption rule, including California state laws protecting the privacy of physical health information, HIV test results, mental health and substance use disorder records; and, 42 CFR Part 2 protections for substance use disorder treatment programs.
6. Any questions related to the pre-emption analysis reflected in the County HIPAA policies and procedures should be directed to the HIPAA Privacy Official or the HIPAA Compliance Committee for resolution, or further action which could include submitting a request to the Secretary of DHHS for an exception to the pre-emption rule.

D. Required Disclosures under HIPAA (45 CFR 164.502; 45 CFR 164.524)

1. If a request is made to any County program or provider by the Secretary of DHHS or designee in relation to an investigation of a breach or other HIPAA-related complaint, or to determine the County's compliance with the HIPAA regulations (45 CFR Subtitle A, Subchapter C), the HIPAA Privacy Officer and/or the HIPAA Compliance Committee shall be promptly notified and shall take the lead in responding to the request.
2. If an individual seeks access to their own PHI that request shall be handled as outlined by the County policy guaranteeing the individual's right to access their own records under HIPAA and California's Patients Access to Health Records Act (see County Privacy and Protected Information Policy, Part 4, Patients' Rights).

E. Permissive Disclosures Under HIPAA and/or More Stringent State or Federal Laws

1. For Treatment, Payment and Operations (45 CFR 164.506)

a. Treatment

1) HIPAA defines treatment at 45 CFR 164.501 to mean "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another."

2) County staff may use, access or disclose PHI for its own treatment purposes subject to the following limitations that narrow the scope of disclosures depending on the nature of the health are records and discipline of the provider that created the PHI:

a) Physical health information may be shared for treatment purposes, as defined by HIPAA and by CMIA for diagnosis and treatment of the patient (California CIV 56.10(c)(1)).

b) Mental health information may be shared for "treatment purposes" only with health care professionals who have "medical or psychological responsibility for the care of the patient" (California WIC 5828(a)(1)).

c) HIV information may be shared for "treatment purposes" when the information is included in the medical chart (California HSC 120980(l), or disclosed to the individual's health care providers for purposes of diagnosis, care or treatment (California HSC 120985).

d) Substance use disorder (SUD) information may only be shared in communications between or among personnel within a County Part 2 substance use disorder treatment program who have a need for the information in connection with their duties that arise out of the provision of diagnosis, treatment, or referral for treatment (42 CFR 2.12(c)(3)); disclosures to other County providers, to other SUD providers in another program, or to other providers in general, all require written consent from the client (42 CFR 2.31 or 2.35) unless the disclosure is necessary in a bona fide medical emergency in which the client's prior informed consent cannot be obtained (42 CFR 2.51).

3. A County provider of physical health care or mental health care may disclose medical information to a county social worker, a probation officer, a foster care public health nurse acting pursuant to Section 16501.3 of the California Welfare and Institutions Code, or any other person who is legally authorized to have custody or care of a minor who is a ward or dependent of the Court, for the purpose of coordinating health care services and medical treatment provided to the minor, including, but not limited to, the sharing of information related to screenings, assessments, and laboratory tests necessary to monitor the administration of psychotropic medications; these disclosures shall not be permitted without the minor's authorization in any case where the minor has the right to consent to the care pursuant to California minor consent

laws (California CIV 56.103; WIC 5828.04).

b. Payment
   1) County staff may use or access PHI for its own payment purposes.
   2) The County may disclose PHI related to physical health care except for HIV test results, to another HIPAA "covered entity" for its payment activities.
   3) The County will not disclose PHI related to HIV test results, mental health care, or SUD treatment to any other covered entity for its payment activities without written authorization from the individual whose PHI is being disclosed.
   4) SUD information may be shared within the County with the entity having direct administrative control over the County Part 2 SUD program for payment purposes.
   5) The "minimum necessary rule" will be followed in all cases when accessing, using or disclosing PHI for payment purposes.

c. Operations
   1) County staff may use or access PHI for its own operation purposes, however only to the extent of the minimally necessary rule to effectively carry out those functions.
   2) The County may disclose PHI related to physical health care, except for HIV test results, to another HIPAA "covered entity" for its operations activities, if that covered entity has or had a relationship with the individual who is the subject of the PHI being requested and the disclosure is limited to:
      a) that entity's healthcare operations, as defined as: "conducting quality assessment and improvement activities, including limited outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; or

      b) for the purpose of health care fraud and abuse detection or compliance.

   3) The County will not disclose PHI related to HIV test results, mental health care, or SUD treatment to any other covered entity for its operations purposes or activities

without written authorization from the individual whose PHI is being disclosed.

4) SUD information may be shared within the County with the entity having direct administrative control over the County Part 2 SUD program for operations purposes.

5) The "minimum necessary rule" will be followed in all cases when accessing, using or disclosing PHI for operations purposes.

2. With Written Authorization

a. Unless otherwise required or permitted by law, and as specified by the County HIPAA policy, written authorization from the individual, also called "consent" under federal confidentiality protections for SUD information (42 CFR Part 2), will be obtained prior to making a disclosure of PHI to an individual or entity.

b. The County authorization form (**Appendix 3**) is HIPAA-compliant and also complies with all other applicable laws; it is the preferred form for obtaining authorization from an individual, but a handwritten authorization that meets HIPAA requirements and complies with CMIA (CIV 56.11) and SUD regulations (42 CFR 2.31 or 2.35) is also acceptable.

c. Forms provided by other providers or entities may only be honored if they meet all of the requirements of HIPAA, CMIA and 42 CFR Part 2 (sections 2.31 or 2.35) and are in 14-point or larger font.

d. The following core elements shall be included on all authorization forms:

1) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

3) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure; if the disclosure includes SUD Part 2 information, the recipient individual or entity must be identified by name unless the disclosure is to a health information exchange in which case the specific requirements of 42 CFR 2.31(a)(4)(ii) should be followed;

4) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;

5) An expiration date or an expiration event or condition that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository; and,

6) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

d. In addition to the above-noted "core elements" the authorization must contain statements to place the individual on notice of all of the following:
   1) The individual's right to revoke the authorization in writing except to the extent that the County has already taken action in reliance upon it, and either:

      a) The exceptions to the right to revoke and a description of how the individual may revoke the authorization (e.g., provision of an address where to send the revocation request); or

      b) To the extent that the information regarding revocation is included in the County Notice of Privacy Practices (NPP), a reference to the County's NPP.

   2) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

      a) The County may not condition treatment, payment, or eligibility for benefits on whether the individual signs the authorization unless an exception applies; or

      b) The consequences to the individual of a refusal to sign the authorization when the County can condition treatment or eligibility for benefits on failure to obtain such authorization.

   3) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by HIPAA or other federal or state laws.

e. Other requirements for written authorization to be valid:
   1) Authorization forms shall be written in plain language;
   2) Authorization forms shall not be combined with other documents (i.e., they will not

be "compound");

3) A separate authorization will be required to permit the disclosure of psychotherapy notes.
4) Authorizations that allow the disclosure of SUD information must describe how much and what kind of SUD information is to be disclosed, including an explicit description of the SUD information that may be disclosed; if SUD information is going to be disclosed to a health information exchange (HIE) for dissemination to members of the HIE, 42 CFR section 2.31(a)(4)(ii) must be followed.
5) Written "consents" (authorizations) that are permitted under 42 CFR Part 2, section 2.35 for individuals involved in criminal justice system referrals are non-revocable under the provisions of that section, which means that they do not satisfy one of the core elements required by HIPAA (revocability); therefore, if a section 2.35 consent is used by the criminal justice system, it is essential that information from the SUD program not be released unless there is also a Court order directing the program to release the information, as specifically provided by the individual on the section 2.35 form.

3. With Verbal Authorization (45 CFR 164.510)

a. Limited information may be disclosed to family, friends or others directly involved in the individual's care, or payment for the individual's care, with verbal permission from the individual, for example, when the patient specifically asks the provider to tell her family member which pharmacy will have the patient's medication and when it is likely to be ready for pick-up; the information shared will be directly related to that other person's involvement in the individual's care or payment for that care and not exceed the "minimum necessary" to achieve that purpose.

b. When information is provided pursuant to verbal authorization a note should be made by the provider or staff in the record indicating that the communication was made and that it was properly authorized by the individual.

c. Any PHI that is shared should not exceed the minimum necessary to communicate the limited information that is needed to accomplish the purpose of the communication.

d. With verbal permission, information regarding the individual's presence at a facility, or admission, discharge or transfer may also be shared at the request of the individual.

e. If the individual is admitted to the psychiatric health facility (PHF) staff should offer to alert someone named by the individual of the fact that they have been admitted; if the

individual does not want anyone to be notified, no information will be shared, for example, if a family member initiates a telephone call to the facility and is seeking information about their loved one. The standard statement that "we can neither confirm nor deny the presence of that person at our facility," would be the proper response to the person making the inquiry when the patient has indicated that they do not want information shared.

f. In a situation where the individual is unable to communicate their wishes regarding family notification, no call will be made to family; however, if a close family member (spouse, parent, child, sibling) contacts the facility, the individual's presence at the facility may be confirmed so long as it is reasonable to do so under the circumstances, and in the health care provider's professional judgment it believed to be in the person's best interest (California WIC 5328.1(a); 45 CFR 164.510(b)(3).

g. In other situations, or any time there is uncertainty about whether a disclosure is permissible or not, the HIPAA Privacy Officer or designated privacy contact within the individual department or program should be consulted.

4. Where No Authorization is Required (45 CFR 164.512)

Note: in any situation where disclosure of PHI to third parties is being considered, staff must first identify the type of information that is going to be disclosed and its source in order to identify and apply the most stringent privacy protections. This is particularly important when HIV test results, mental health information, or substance use disorder treatment program information is the PHI under consideration since these types of information are often subject to more stringent rules than HIPAA would provide.

The following disclosures are permitted under HIPAA, but may be subject to more stringent privacy laws and limitations, which will be also be discussed. Any time a disclosure does not fall squarely under one of these subsections, staff is cautioned to check with their chain of command, or with the County HIPAA Privacy Officer prior to making the disclosure.

When physical health information is involved, the "more stringent" test does not usually limit the HIPAA-permitted disclosure because of provisions in the California Confidentiality of Medical Information Act (CMIA): CMIA requires, at Civil Code 56.10(b)(7), the disclosure of confidential health information in cases where another law requires the disclosure (e.g., to the Secretary of DHHS investigating a HIPAA breach), and permits, at Civil Code 56.10(c)(14), the disclosure of physical health information if another law "authorizes" it; HIPAA is another such law, so disclosures authorized by HIPAA would be permitted by CMIA.

a. If Required by Law - HIPAA permits the disclosure of PHI to the extent that such use or disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law; these permissive disclosures are further limited by HIPAA regulations permitting the reporting of various forms of abuse, rules related to judicial and administrative hearings, and disclosures to law enforcement, which are discussed in sections "c," "e," and "f" below. Generally, this permissive disclosure of PHI does not allow for the acknowledgement that an individual is a patient receiving SUD treatment unless specifically allowed by 42 CFR Part 2; for example, a Tarasoff warning the is "required by law" needs to be given in such a way that neither the provider nor the client are linked to the SUD Program.

b. For Public Health Activities

1) For Public Health and Medical Safety

a) County health care providers may disclose PHI to a public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations and public health interventions.

b) Disclosure may also be made to a person exposed to a communicable disease or who may otherwise be at risk of contracting or spreading a disease or condition if the County or public health authority is authorized by law to make this disclosure as necessary in the conduct of a public health intervention or investigation.

c) Reports may be made to the Food and Drug Administration with respect to an FDA-regulated product or activity for purposes related to the quality, safety or effectiveness of such FDA-regulated product or activity.

d) Disclosures may also be made to schools related to proof of immunization where the school is required by the state to have that proof and the parent/legal guardian or individual with consent rights agrees to that disclosure.

2) Reports of Child Abuse - HIPAA permits reports of child abuse to the public health authority or other appropriate government authority authorized by law to receive mandated reports of child abuse or neglect.

c. Victims of Elder/Dependent Adult Abuse/Neglect

1) HIPAA permits the disclosure of PHI when County health care staff who are mandated reporters for elder and dependent adult abuse and neglect must file a report as required under California's elder and dependent adult abuse and neglect

mandating reporting laws. The disclosure of PHI is permitted to the extent that it is required and is limited to the relevant requirements of the law, or if the individual agrees to the disclosure, or if the County health care provider believes, in the exercise of professional judgement, that the disclosure is necessary to prevent serious harm to the individual whose PHI is disclosed or to other potential victims.

2) HIPAA requires the County to promptly notify the individual that such a report has been or will be made unless the provider, in the exercise of professional judgment, believes that informing the individual would place the individual at risk of serious harm or, in cases involving informing a personal representative, where the provider reasonably believes that the personal representative is responsible for the abuse, neglect, or other injury and that informing such person would not be in the best interests of the patient.

d. Health Oversight/Licensing

1) The County may use, or disclose PHI to a health oversight agency, for oversight activities authorized by law, including audits; civil, administrative or criminal investigations, proceedings or actions; licensure or disciplinary actions; or other activities necessary for the appropriate oversight of the healthcare system, benefit programs where PHI is relevant to beneficiary eligibility, regulatory programs where PHI is necessary for determining compliance with program standards, or where PHI is necessary for determining compliance with civil rights laws applicable to the health care entity.

2) Health oversight disclosures do not include investigations or other activities where the individual is the subject of the investigation or activity and the investigation or activity does not arise out of and is directly related to the receipt of health care, a claim for public benefits related to health or qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

e. Judicial and Administrative Proceedings

1) HIPAA permits the County to disclose PHI in the course of any judicial or administrative proceeding in response to an order of a court or administrative tribunal so long as the disclosure is limited to the PHI expressly authorized by the order. Court orders requiring the disclosure of SUD information should follow the strict rules found in 42 CFR Part 2, sections 2.61-2.67.

2) HIPAA permits disclosure of PHI in response to a subpoena, discovery request, or other lawful process that is not accompanied by a court or administrative tribunal order if the County receives satisfactory assurances that the party seeking the information has made reasonable efforts to ensure that the individual has been given notice or that the party seeking the information has made reasonable efforts to secure a qualified protective order from the court or tribunal.

   a) Satisfactory assurances re: notice to the individual include a written statement and accompanying documentation demonstrating that the party requesting the information has made a good faith attempt to provide written notice to the individual at the individual's last known address and that the notice contained sufficient information about the litigation or proceeding to permit the individual raise an objection in the proper forum and that the time to raise an objection has elapsed and either no objections were filed, or any that were filed have been resolved by the court or tribunal and the disclosures being sought are consistent with such resolution.

   b) Satisfactory assurances re: securing of a qualified protective order means obtaining an order or stipulation by the parties that prohibits the use or disclosure of the PHI for any purpose other than the litigation or proceeding for which such information was requested and requires the return or destruction of the PHI at the end of the litigation or proceeding.

3) Alternatively, the County can make its own reasonable efforts to provide notice or seek a qualified protective order and proceed once that notice is provided, and adequate time has passed, or an order is agreed to and presented to the court or obtained from the court.

4) A subpoena alone is not sufficient to support the disclosure of HIV test results, mental health information, or SUD treatment program information. It must be accompanied either by

   a) a Court order directing the delivery the information to the Court as necessary to the administration of justice, or

   b) written authorization/consent from the patient.

f. Law Enforcement

1) HIPAA and state law permit the disclosure of PHI to law enforcement if required by laws that require a report from a health care provider providing medical care to a person suffering from a wound or injury caused by gunshot, including self-inflicted or accidental wounds, or by assaultive or abusive conduct.

   a) This exception to privacy would apply in public health, clinic, and hospital settings where medical care for physical conditions is provided and where physical health privacy laws apply.
   b) Disclosures to law enforcement in response to a court order or court-ordered and signed warrant or a subpoena or summons issued by a judicial officer or a grand jury subpoena or an administrative request all potentially raise issues, depending on the type of information sought; the employee who receives the warrant, subpoena or summons should seek guidance from the HIPAA Privacy Official or from the Office of County Counsel in these situations.

2) Limited information may be shared with law enforcement for the purpose of locating a suspect, fugitive, material witness, or missing person, provided that only the following information be disclosed: name and address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, if applicable, and a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars and tattoos. Note that only physical health care providers could share this information under CMIA, since more stringent laws that apply to mental health and SUD information do not permit this type of disclosure without authorization from the client. Note that in some cases if an individual is missing from a locked mental health facility this information may be shared, but it is subject to different rules. If the County behavioral health staff is aware of a missing person report, the County health provider or program may notify the individual directly of this fact so that the individual can authorize the disclosure, or contact law enforcement themselves, directly.

3) Protected health information may be disclosed in response to a law enforcement official's request for such information if the individual is or is suspected to be a victim of a crime and the individual agrees to the disclosure. If authorization for the disclosure cannot be obtained because of incapacity or other emergency

circumstance, staff should contact the HIPAA Privacy Officer or Office of County Counsel for guidance per the exceptions outlined in 45 CFR 164.512(f)(3)(ii).

4) Decedents - PHI may be disclosed to law enforcement if the County believes that the individual's death may have resulted from criminal conduct; this would most likely involve disclosures of physical health information and therefore no disclosure of mental health or SUD information should be made without guidance from the HIPAA Privacy Officer.

5) Crime on Premises - PHI may be disclosed to a law enforcement official if County staff believe in good faith that it is necessary to share the information as evidence of criminal conduct on the premises of the facility where health care services are provided. This HIPAA exception to confidentiality allows limited disclosure of PHI in all physical health care settings, and it is permitted under California mental health and federal SUD confidentiality laws as well if necessary to get help when a crime is committed or threatened against the staff or premises of behavioral health programs.

6) Reporting Crime in Emergencies - County staff and first responders providing emergency health care in response to a medical emergency, other than emergencies on County premises, may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement about the commission and nature of a crime, the location of such crime or victims of such crime, and the identity, description and location of the perpetrator of such crime. It the crime involves reportable abuse or neglect, this section would not apply and the rules regarding mandated reporting should be followed.

g. Decedents

1) The County may disclose physical health information to a coroner or medical examiner for the purpose of identifying a deceased purpose, determine a cause of death, or other duties as authorized by law.

2) The County may also disclose physical health information to funeral directors as necessary to carry out their duties, and if necessary may disclose the information prior to, and in reasonable anticipation of the individual's death.

3) HIV, mental health and SUD information should not be disclosed about decedents without first seeking direction from the HIPAA Privacy Officer.

h. Organ/Tissue Donation

1) The County may use or disclose physical health information to a organ procurement organization or other entity engaged in the procurement, banking or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

2) Before making disclosures without authorization from the patient or patient representative, staff should check with their chain of command or the HIPAA Privacy Officer for guidance.

i. Research

1) The County may disclose PHI for research provided that it has documentation that there is an alteration to or waiver in whole or in part of the individual authorization requirements normally needed prior to the disclosure of PHI, and that it has been approved by an Institutional Review Board (IRB) established in accordance with federal laws and regulations, or a privacy board as specified by law.

2) Alternatively, the County may obtain from the researcher representations that the use or disclosure is sought solely to prepare a research protocol and no PHI will be removed from the premises of the County health facility, and that the limited PHI that is reviewed is necessary for research purposes.

3) If the research is on a decedent's PHI, the County shall first obtain from the researcher that the use or disclosure is solely for research on the PHI of decedents and that the researcher provide documentation of the death of such individuals, and representations that the PHI is necessary for research purposes.

4) Because the documentation requirements will vary for each project, no PHI shall be disclosed to a researcher or for research purposes without first seeking guidance from the HIPAA Privacy Official, who will determine if proper documentation has been obtained and prepared to the satisfaction of the County and as required by law.

j. To Avert a Threat to Health or Safety

1) The County may disclose PHI if it believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is made to a person or persons reasonably able to

prevent or lessen the threat, including the target of the threat or is necessary for law enforcement authorities to identify or apprehend an individual.

2) The Tarasoff "duty to warn" is triggered when a patient communicates a serious threat against a reasonably identifiable victim or victims to a psychotherapist, who then discharges their duty to warn by notifying the victim(s) if the psychotherapist can reasonably do that, and to law enforcement. Because the Tarasoff "duty to warn" is required by law, it is already a HIPAA exception (the first listed in this section) but in some cases may also fall under this HIPAA exception to confidentiality. Regardless of where it falls, good documentation as to the rationale for the clinical decision to warn or to not warn is essential. The minimum necessary amount of information to adequately convey the seriousness of the threat may vary upon the circumstances and response of the intended victim. If the psychotherapist is working in an SUD program, the warning must not include any information that would link either the therapist or the client to the SUD program. After providing their name and type of professional licensure (e.g., LCSW or MFT), the psychotherapist can merely state, "I work for County Behavioral Health" which avoids stating the specific program the therapist works in and disclosing SUD information that is protected.

3) The disclosure of PHI permitted under this section of HIPAA includes disclosures when an individual has escaped from a correctional institution or from lawful custody.

4) The exception permitting the disclosure of PHI to lessen a threat to public health or safety also requires that County staff act in good faith with regard to the belief that the disclosure is necessary to lessen the threat, and reliance on credible representations by persons with apparent knowledge or authority.

k. Specialized Government Functions

1) In all cases where PHI is sought for the following specialized government functions, County staff shall immediately notify the HIPAA Privacy Official and/or the Office of County Counsel and seek guidance in the specific situations:

   a) Requests from representatives of the military seeking PHI of individuals who are Armed Forces personnel made by appropriate military command authorities for specific lawful purposes; similar requests might be made by

foreign military authorities seek PHI of foreign military personnel and may be permitted as exceptions to privacy.

b) PHI that is requested by authorized federal officials for lawful activities authorized by the National Security Act and implementing authority, or to the Secret Service for the protection of the President and other constitutionally elected officials and their families, or to protect foreign heads of state and their families.

c) Requests from correctional institutions or law enforcement officials having lawful custody of an inmate where the information is needed for a reason other than treatment purposes by correctional care staff, or for coordination of care between the correctional care staff and outside healthcare providers; generally information may be shared for the health and safety of individuals, other inmates, officers and employees of the correctional institution and others responsible for transporting inmates or transferring inmates from one institution to another, or to medical appointments outside the correctional facility.

2) The routine reporting at discharge to the California Department of Justice of individuals who were admitted involuntarily (WIC 5151) into the psychiatric health facility as “danger to self” or “danger to others” for the purpose of triggering appropriate firearms prohibitions under California WIC 8100 et seq. is an exception to both HIPAA and the LPS Act confidentiality laws; this reporting is done at discharge of these individuals, and may be done by staff trained specifically on the protocol for reporting to the Department of Justice. Training shall include the proper documentation requirements, and protocol for notification to the patient of the report with information on how to petition the court for relief from the firearms prohibition (Form BOF 4009C).

I. Workers’ Compensation

1) HIPAA permits the disclosure of PHI as authorized by and to the extent necessary to comply with laws relating to workers’ compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

2) HIV, mental health and SUD information should not be disclosed without written authorization/consent from the individual.

2.3. REFERENCES

HIPAA - 45 CFR Parts 160 and 164
SUD Confidentiality - 42 CFR Part 2
CMIA - California Civil Code 56.10 et seq.
PAHRA - California Health and Safety Code 123100 et seq.
HIV - California Health and Safety Code 120980, 120985
LPS Act - California Welfare and Institutions Code 5000 et seq.

Part 3 - Security Rule

3.1 PURPOSE

A. The purpose of this policy is to provide guidance to staff and clear direction on the County of El Dorado's responsibility to maintain and ensure the confidentiality, security, integrity and availability of all protected health information ("PHI") or Medi-Cal personally identifiable information (PII) that it creates, receives, maintains or transmits.
B. The guidance provided in this policy shall also apply to all contractors and vendors who use, access, or maintain PHI on behalf of the County in their roles as business associates and any business associate agreement with them shall specifically require that the business associate implement and adhere to the HIPAA Security Rule and related standards to assure the security of any PHI or ePHI the business associate uses, creates, accesses, maintains or discloses.
C. The County shall take all reasonable steps to protect against reasonably anticipated threats or hazards to the security or integrity of any electronic protected health information (ePHI) it creates, receives, maintains or transmits.
D. The County shall protect against any reasonably anticipated uses or disclosures of all PHI and ePHI that are not permitted under the law or the County Privacy and Protected Information Policy and shall take steps to ensure compliance by its workforce and business associates.
E. The County shall implement these security policies and procedures to prevent, detect, contain and correct security violations

3.2 POLICY

A. General Security Rule.

1. The County shall have in place appropriate administrative, technical, and physical safeguards to protect the security of protected health information, both PHI and ePHI.
2. These safeguards will be designed to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of federal or state medical privacy laws.

3. The County will reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.
4. In implementing security standards, the County shall implement all "required" standards and will assess and implement, when reasonable and appropriate, all "addressable implementation standards" included in the HIPAA Security Rule (45 CFR Part 164, Subpart C). Any decision to not implement an addressable standard will be documented with the reason why it would not be reasonable and appropriate to adopt it as specified, as well as a description of any equivalent alternative measure that is reasonable and appropriate, and that is adopted.
5. The County will review and modify the security measures implemented by this policy as needed on a continuing basis to assure the provision of reasonable and appropriate protection of PHI and ePHI and will update these measures as necessary.

B. Definitions

As used in this policy, the following terms have the following meanings:

1. **Access** means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

2. **Administrative safeguards** are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the County's or a business associate's workforce in relation to the protection of that information.

3. **Assist in the administration of the Medi-Cal program** means performing administrative functions on behalf of Medi-Cal, such as establishing eligibility, determining the amount of medical assistance, and collecting Medi-Cal PII for such purposes, to the extent such activities are authorized by law.

4. **Authentication** means the corroboration that a person is the one claimed.

5. **Availability** means the property that data or information is accessible and useable upon demand by an authorized person.

6. **Breach** refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for other than authorized purposes, have

access or potential access to PHI or Medi-Cal PII, whether electronic, paper, verbal, or recorded.

7. **Confidentiality** means the property that data or information is not made available or disclosed to unauthorized persons or processes.

8. **County Worker** means those county employees, contractors, subcontractors, vendors and agents performing any functions for the County that require access to and/or use of Medi-Cal PII and that are authorized by the County to access and use PHI and Medi-Cal PII.

9. **Encryption** means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

10. **Facility** means the physical premises and the interior and exterior of a building(s).

11. **Information system** means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

12. **Integrity** means the property that data or information have not been altered or destroyed in an unauthorized manner.

13. **Malicious software** means software, for example, a virus, designed to damage or disrupt a system.

14. **Medi-Cal PII** is personally identifiable information directly obtained in the course of performing an administrative function on behalf of Medi-Cal that can be used alone, or in conjunction with any other information, to identify a specific individual. Medi-Cal PII includes any information that can be used to search for or identify individuals, or can be used to access their files, including but not limited to name, social security number (SSN), date and place of birth (DOB), mother's maiden name, driver's license number, or identification number. Medi-Cal PII may also include any information that is linkable to an individual, such as medical, educational, financial, and employment information. Medi-Cal

PII may be electronic, paper, verbal, or recorded and includes statements made by, or attributed to, the individual.

15. **Password** means confidential authentication information composed of a string of characters.

16. **Physical safeguards** are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

17. **Secure Areas** means any areas where:
    a. County Workers assist in the administration of Medi-Cal;
    b. County Workers use or disclose Medi-Cal PII; or
    c. Medi-Cal PII is stored in paper or electronic format.

18. **Security or Security measures** encompass all of the administrative, physical, and technical safeguards in an information system.

19. **Security incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

20. **SSA-provided or verified data (SSA data)** means:
    a. Any information under the control of the Social Security Administration (SSA) provided to DHCS under the terms of an information exchange agreement with SSA (e.g., SSA provided date of death, SSA Title II or Title XVI benefit and eligibility data, or SSA citizenship verification); or
    b. Any information provided to DHCS, including a source other than SSA, but in which DHCS attests that SSA verified it, or couples the information with data from SSA to certify the accuracy of it (e.g. SSN and associated SSA verification indicator displayed together on a screen, file, or report, or DOB and associated SSA verification indicator displayed together on a screen, file, or report).

21. **Technical safeguards** means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

22. **User** means a person or entity with authorized access.

23. **Workstation** means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

C. Administrative Safeguards (45 CFR 164.308)

To ensure compliance with applicable privacy and security safeguards the County shall do the following and assure that its business associates follow similar practices:

1. Security Management Process

a. Risk analysis (required) - The County shall conduct and document an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the County.

b. Risk management (required). The County shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule

c. Sanction policy (required). The County shall apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. If there is a violation of policy, whether intentional, reckless, negligent or accidental, appropriate chain of command and human resources staff will be notified and involved in implementing and applying sanctions against the employee. If the violation involves a business associate, the County HIPAA Security Officer will be immediately notified, and the HIPAA Security Officer will involve the Office of County Counsel as appropriate to the circumstances.

d. Information system activity review (required). The County Security Officer will implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports, and will document activities related to this system review.

2. Assigned Security Responsibility

a. The County HIPAA Security Officer shall be responsible for the review, development and implementation of the policies and procedures necessary to assure compliance with the

HIPAA Security Rule.

b. The County HIPAA Security Officer shall report to the County HIPAA Compliance Committee on a regular basis.

3. Workforce security.

The County will ensure that all members of its workforce have appropriate access to electronic protected health information, as necessary to perform their jobs.

a. Authorization and/or supervision (addressable). The County will implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

b. Workforce clearance procedure (addressable). The County will implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

c. Termination procedures (addressable). The County will implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by a change in work responsibilities or other changed situation. For example, when an employee is terminated or voluntarily leaves County employment, password access will immediately be blocked, and all passwords for inhouse as well as all outside programs and memberships, devices and media will be turned in through the chain of command, as appropriate to the situation.

4. Information access management.

a. Isolating health care clearinghouse functions (required). If a clearinghouse function ever becomes part of County operations, its ePHI will be separated from other County functions to protect it from unauthorized access.

b. Access authorization (addressable). The County will grant access to appropriate staff to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. Job descriptions will reflect job duties that require access to PHI and ePHI.

c. Access establishment and modification (addressable). The County HIPAA Security Officer together with an employee's chain of command, will establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process as appropriate to their job duties.

5. Security awareness and training.

a. Security reminders (addressable). Periodic security updates will be sent to appropriate staff on a regular basis by the HIPAA Security Officer.

b. Protection from malicious software (addressable). The HIPAA Security Officer shall be responsible for implementing procedures for guarding against, detecting, and reporting malicious software.

c. Log-in monitoring (addressable). The HIPAA Security Officer shall be responsible for implementing procedures for monitoring log-in attempts and documenting and reporting discrepancies.

d. Password management (addressable). The HIPAA Security Officer shall be responsible for implementing procedures for creating, changing, and safeguarding passwords and will monitor compliance by the workforce.

6. Security incident procedures.

a. The County HIPAA Security Officer shall implement appropriate protocols to address security incidents.

b. Response and reporting (required). The County HIPAA Security Officer shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the County; and document security incidents and their outcomes.

7. Contingency plan. The County HIPAA Security Officer shall establish (and implement as needed) protocols for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

a. Data backup plan (required). The County HIPAA Security Officer shall establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

b. Disaster recovery plan (required). The County HIPAA Security Officer shall establish (and implement as needed) procedures to restore any loss of data.

c. Emergency mode operation plan (required). The County HIPAA Security Officer shall establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

d. Testing and revision procedures (addressable). The County HIPAA Security Officer shall implement procedures for periodic testing and revision of contingency plans.

e. Applications and data criticality analysis (addressable). The County HIPAA Security Officer shall assess the relative criticality of specific applications and data in support of other contingency plan components.

8. Evaluation. The County HIPAA Security Officer shall perform a periodic technical and nontechnical evaluation, based initially upon the standards listed in this policy that reflect the HIPAA Security Rule standards, and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that assure that the County's security policies and procedures meet the requirements of that Rule.

a. Business associate contracts and other arrangements. The County may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances in a business associate agreement or other contractual promises that the business associate will appropriately safeguard any County PHI.

b. Written contract or other arrangement (required). The County HIPAA Security Officer will work with the Office of County Counsel to make sure appropriate language is included in business associate agreements to assure compliance with the HIPAA Security Rule.

9. Personnel Controls - Medi-Cal PII. The County will advise County Workers who have access to Medi-Cal PII, of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable federal and state laws. For that purpose, the County Department/Agency shall implement the following personnel controls:

a. **Employee Training.** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by County Workers, including, but not limited to:
   1) Provide initial privacy and security awareness training to each new County Worker within 30 days of employment;
   2) Thereafter, provide annual refresher training or reminders of the privacy and security safeguards to all County Workers (California state DHCS recommends three or more security reminders per year);
   3) Maintain records indicating each County Worker's name and the date on which the privacy and security awareness training was completed and;
   4) Retain training records for a period of three years after completion of the training.

b. Employee Discipline.

   1) Maintain documented sanction policies and procedures for County Workers who fail to comply with privacy policies and procedures or any provisions of these requirements.

   2) Sanction policies and procedures shall include termination of employment when appropriate.

c. Confidentiality Statement. Ensure that all County Workers sign a confidentiality statement. The statement shall be signed by County Workers prior to accessing Medi-Cal PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of three years, or five years if the signed statement is being used to comply with Section 5.10 of the SSA's "Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA" document. The statement, at a minimum, shall include:

   1) General use of Medi-Cal PII;

   2) Security and Privacy safeguards for Medi-Cal PII;

   3) Unacceptable use of Medi-Cal PII; and,

4) Enforcement policies.

d. Background screening.

1) Conduct a background screening of a County Worker before they may access Medi-Cal PII.

2) The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those employees who are authorized to bypass significant technical and operational security controls.

3) The County shall retain each County Worker's background screening documentation for a period of three years following conclusion of employment relationship.

D. Physical Safeguards

1. Facility access controls. The County HIPAA Security Officer shall implement protocols to limit physical access to its electronic information systems and the County facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

a. *Contingency operations (addressable).* The County HIPAA Security Officer shall establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

b. *Facility security plan (addressable).* The County HIPAA Security Officer shall implement protocols to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

c. *Access control and validation procedures (addressable).* The County HIPAA Security Officer shall implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

d. *Maintenance records (addressable).* The County HIPAA Security Officer shall document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

2. ***Workstation use.*** The County HIPAA Security Officer shall implement protocols that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

3. ***Workstation security.*** *T*he County HIPAA Security Officer shall Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

4. ***Device and media controls.*** The County HIPAA Security Officer shall Implement protocols that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a County facility, and the movement of these items within a County facility.

   a. *Disposal (required).* The County HIPAA Security Officer shall Implement protocols to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

   b. *Media re-use (required).* The County HIPAA Security Officer shall Implement protocols for removal of electronic protected health information from electronic media before the media are made available for re-use.

   c. *Accountability (addressable).* The County HIPAA Security Officer shall maintain a record of the movements of hardware and electronic media and any person responsible, therefore.

   d. *Data backup and storage (addressable).* The County HIPAA Security Officer shall create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

5. **Physical Security - Medi-Cal PII.** The County shall ensure Medi-Cal PII is used and stored in an area that is physically safe from access by unauthorized persons at all times. The

County shall safeguard Medi-Cal PII from loss, theft, or inadvertent disclosure and, will do the following:

a. Secure all areas of the County facilities where County Workers assist in the administration of Medi-Cal and use, disclose, or store Medi-Cal PII.

b. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:
    1. Properly coded key cards;
    2. Authorized door keys; and,
    3. Official identification.

c. Issue identification badges to County Workers.

d. Require County Workers to wear these badges where Medi-Cal Pll is used, disclosed, or stored.

e. Ensure each physical location where Medi-Cal PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.

f. Ensure there are security guards or a monitored alarm system at all times at County facilities and leased facilities where 500 or more individually identifiable records of Medi-Cal PII is used, disclosed, or stored. Video surveillance systems are recommended.

g. Ensure that data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of Medi-Cal PII have perimeter security and physical access controls that limit access to only authorized County Workers. Visitors to the data center area shall be escorted at all times by authorized County Workers.

h. Store paper records with Medi-Cal PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use, meaning that there are County and non-County functions in one building in work areas

that are not securely segregated from each other. It is recommended that all Medi-Cal PII be locked up when unattended at any time, not just within multi-use facilities.

I. The County shall have policies based on applicable factors that include, at a minimum, a description of the circumstances under which the County Workers can transport Medi-Cal PII, as well as the physical security requirements during transport. If the County chooses to permit its County Workers to leave records unattended in vehicles, it shall include provisions in its policies to provide that the Medi-Cal PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances may Medi-Cal PII be left unattended in a vehicle overnight or for other extended periods of time.

i. The County shall have policies that indicate County Workers are not to leave records with Medi-Cal PII unattended at any time in airplanes, buses, trains, etc., inclusive of baggage areas. This should be included in training due to the nature of the risk.

6. Medi-Cal PII - Paper Document Controls

a. Supervision of Data. Medi-Cal PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information.

b. Data in Vehicles. The County shall have policies that include, based on applicable risk factors, a description of the circumstances under which the County Workers can transport Medi-Cal PII, as well as the physical security requirements during transport. If the County decides to permit its County Workers to leave records unattended in vehicles, it shall include provisions in its policies to provide that the Medi-Cal PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit Medi-Cal PII to be left unattended in a vehicle overnight or for other extended periods of time.

c. Public Modes of Transportation. Medi-Cal PII in paper form shall not be left unattended at any time in airplanes, buses, trains, etc., inclusive of baggage areas. This should be included in training due to the nature of the risk.

d. Escorting Visitors. Visitors to areas where Medi-Cal PII is contained shall be escorted, and Medi-Cal PII shall be kept out of sight while visitors are in the area.

e. Confidential Destruction. Medi-Cal PII shall be disposed of through confidential means, such as crosscut shredding or pulverizing.

f. Removal of Data. Medi-Cal PII shall not be removed from the premises of County Department/Agency except for justifiable business purposes.

g. Faxing.

1) Faxes containing Medi-Cal PII shall not be left unattended and fax machines shall be in secure areas.

2) Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.

3) Fax numbers shall be verified with the intended recipient before sending the fax.

h. Mailing.

1) Mailings containing Medi-Cal PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.

2) Mailings that include 500 or more individually identifiable records containing Medi-Cal PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt.

E. Technical Safeguards

1. Access control. The County HIPAA Security Officer shall implement technical protocols for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights based upon their job description.

a. Unique user identification (required). The County HIPAA Security Officer shall assign a unique name and/or number for identifying and tracking user identity.

b. Emergency access procedure (required). The County HIPAA Security Officer shall establish (and implement as needed) protocols for obtaining necessary electronic protected health information during an emergency.

c. Automatic logoff (addressable). The County HIPAA Security Officer shall implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

d. Encryption and decryption (addressable). The County HIPAA Security Officer shall implement a mechanism to encrypt and decrypt electronic protected health information.

2. **Audit Controls.** The County HIPAA Security Officer shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

3. **Integrity.**

a. The County HIPAA Security Officer shall implement protocols to protect electronic protected health information from improper alteration or destruction**.**

b. Mechanisms to authenticate electronic protected health information (addressable). The County HIPAA Security Officer shall implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

4. **Person or entity authentication.** The County HIPAA Security Officer shall implement protocols to verify that a person or entity seeking access to electronic protected health information is the one claimed.

5. Transmission security.

a. The County HIPAA Security Officer shall implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

b. Integrity controls (addressable). The County HIPAA Security Officer shall implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

c. Encryption (addressable). The County HIPAA Security Officer shall implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

6. Technical Safeguards - Medi-Cal Electronic PII

a. Workstation/Laptop Encryption. All workstations and laptops, which use, store and/or process Medi-Cal PII, shall be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution shall be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.

b. Server Security. Servers containing unencrypted Medi-Cal PII shall have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

c. Minimum Necessary. Only the minimum necessary amount of Medi-Cal PII required to perform required business functions may be accessed, copied, downloaded, or exported.

d. Mobile Device and Removable Media. All electronic files which contain Medi-Cal PII shall be encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption shall be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.

d. Antivirus Software. All workstations, laptops and other systems, which process and/or store Medi-Cal PII, shall install and actively use an anti-virus software solution. Anti-virus software should have automatic updates for definitions scheduled at least daily.

e. Patch Management.

1) All workstations, laptops and other systems, which process and/or store Medi-Cal PII, shall have critical security patches applied, with system reboot if necessary.

2) There shall be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.

3) At a maximum, all applicable patches deemed as critical shall be installed within 30 days of vendor release. It is recommended that critical patches which are high risk be installed within 7 days.

4) Applications and systems that cannot be patched within this timeframe, due to significant operational reasons, shall have compensatory controls implemented to minimize risk.

f. User IDs and Password Controls.

1) All users shall be issued a unique username for accessing Medi-Cal PII.
2) Usernames shall be promptly disabled, deleted, or the password changed within, at most, 24 hours of the transfer or termination of an employee.

3) Passwords are not to be shared.

4) Passwords shall be at least eight characters.

5) Passwords shall be a non-dictionary word.

6) Passwords shall not be stored in readable format on the computer or server.

7) Passwords shall be changed every 90 days or less. It is recommended that passwords be required to be changed every 60 days or less. Non-expiring passwords are permitted when in full compliance with NIST SP 800-63B Authenticator Assurance Level (AAL) 2.

8) Passwords shall be changed if revealed or compromised.

9) Passwords shall be composed of characters from at least three of the four groups from the standard keyboard:
   a) Upper case letters (A-Z)

   b) Lower case letters (a-z)

   c) Arabic numerals (0-9)

   d) Special characters

g. User Access. In conjunction with DHCS, management should exercise control and oversight, of the function of authorizing individual user access to SSA data via Medi-Cal Eligibility Data System (MEDS), and over the process of issuing and maintaining access control numbers, IDs, and passwords.

h. Data Destruction. When no longer needed, all Medi-Cal PII shall be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the Medi-Cal PII cannot be retrieved.

i. System Timeout. The systems providing access to Medi-Cal PII shall provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

j. Warning Banners. The systems providing access to Medi-Cal PII shall display a warning banner stating, at a minimum:

1) Data is confidential;

2) Systems are logged;

3) System use is for business purposes only, by authorized users; and

4) Users shall log off the system immediately if they do not agree with these requirements.

k. System Logging.

1) The systems that provide access to Medi-Cal PII shall maintain an automated audit trail that can identify the user or system process which initiates a request for Medi-Cal PII, or alters Medi-Cal PII.

2) The audit trail shall:

a) Be date and time stamped;

b) Log both successful and failed accesses;

c) Be read-access only; and

d) Be restricted to authorized users of the audit trail.

3) If Medi-Cal PII is stored in a database, database logging functionality shall be enabled.

4) Audit trail data shall be archived for at least three years from the occurrence.

l. Access Controls. The system providing access to Medi-Cal PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.

m. Transmission Encryption.

1) All data transmissions of Medi-Cal PII outside of a secure internal network shall be encrypted using a FIPS 140-2 certified algorithm that is 128 bit or higher, such as AES or TLS. It is encouraged, when available and when feasible, that 256 bit encryption be used.

2) Encryption can be end to end at the network level, or the data files containing Medi-Cal PII can be encrypted.

3) This requirement pertains to any type of Medi-Cal PII in motion such as website access, file transfer, and email.

n. Intrusion Prevention. All systems involved in accessing, storing, transporting, and protecting Medi-Cal PII, which are accessible through the Internet, shall be protected by an intrusion detection and prevention solution.

F. Organizational requirements (Business Associate Contracts)

1. The HIPAA Security Officer shall verify with the department or Office of County Counsel that all business associates have executed an agreement or contract that specifies the business associate's responsibility to meet all requirements of the HIPAA Security Rule and Medi-Cal PII privacy and security rules.

2. The business associate shall be required to promptly notify the County of any breach or other security incident, and to take immediate steps to cure the breach or take action regarding the incident as appropriate.

3. The County will terminate any contract with a business associate if it knows of a pattern of activity or practice that constitutes a material breach of the business associate's obligation under the contract to follow that requirements of the HIPAA Security Rule and the breach or violation is not able to be cured.

G. Policies and Procedures and Documentation Requirements

1. The County HIPAA Security Officer shall implement reasonable and appropriate protocols to assure compliance with the HIPAA Security Rule; those protocols, and related policies and procedures, may be updated or changed at any time, provided the changes are documented and are in compliance with the HIPAA Security Rules

2. The County HIPAA Security Officer shall maintain documentation reflecting the policies, procedures and protocols that have been implemented in order to comply with the HIPAA Security Rule, and shall maintain a written record of all actions, activities and assessments of actions under these policies, procedures and protocols.

3. The County shall retain documentation reflecting compliance with the HIPAA Security rule for at least six (6) years from the date of implementation of a policy, procedure or protocol, or from the date when it was last in effect, whichever is later.

4. The County shall make its documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

5. The County HIPAA Security Officer shall review the policies, procedures, protocols and documentation practices periodically, and update them as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

3.3 REFERENCES

HIPAA

45 CFR Part 160
45 CFR Part 164, Subpart E, §164.530(c)
45 CFR Part 164, Subpart C - Security Standards for the Protection of Electronic Protected Health Information

DHCS All County Letter #19-16 (June 21, 2019)
2019 Medi-Cal Privacy and Security Agreement (PSA)

4.0 CONSUMER RIGHTS

4.1 PURPOSE

A. The purpose of this policy is to provide guidance to staff regarding the rights of individuals that are provided by the Health Insurance Portability and Accountability Act (HIPAA), the California Patient Access to Health Records Act (PAHRA), and other federal and state laws protecting and providing rights to individuals who receive healthcare services from the County of El Dorado (County).

B. Any rights afforded an individual patient under this policy are rights that the patient representative can exert on behalf of the patient in their role as the patient representative and in the same manner as the patient, unless specifically limited or modified by law.

C. The rights included in this policy include the right to receive a Notice of Privacy Practices, the right to request special privacy protections for protected health information (PHI), the right to request alternative means or places for communications from the County, the individual's right

to access their own PHI, the right to amend inaccurate or incomplete PHI created by the County and to add an addendum to the record, and the right to an accounting of disclosures of the PHI.

D. Additional rights are discussed in other Parts of the County's Privacy and Protected Information Policy, including the right of an individual to submit a complaint or report a concern if they believe their PHI has been improperly used or disclosed by the County (see Part 1 - Administration), and the right to be notified in the case of a breach (see Part 5 - Breach Reporting).

4.2 POLICY

A. Right to Receive a Notice of Privacy Practices (45 CFR 164.520)

1. An individual who receives healthcare services from the County has a right to adequate notice of the uses and disclosures of their PHI that may be made by the County, as well as their own rights and the County's duties with respect to their PHI. Note that an individual detained in the County Jail or the County Juvenile Detention Facility does not have the right to receive the Notice of Privacy Practices during their incarceration but can request and will receive a copy once released.

2. Upon first service delivery, whether in person or via telehealth, Consumers receiving services from the County shall be offered a copy of the "Notice of Privacy Practices" (NPP) (Appendix 9). The copy may be given to them in person, or alternatively, if services are first delivered via telehealth, the Notice may be sent electronically via email, or via USPS mail; it may then also be offered to the individual "in person" when an in person visit occurs.

3. Individuals may receive additional copies of the NPP upon request. In an emergency treatment situation, the Notice shall be provided as soon as practicable following the emergency treatment situation.

4. Employees providing health services shall make a good faith effort to obtain written acknowledgment of receipt of the notice. If the signed Acknowledgement of Receipt of the Notice of Privacy Practices (Appendix 10) is not obtained, staff shall document the good faith efforts to obtain such acknowledgment and the reason why acknowledgment was not obtained.

5. The signed Acknowledgment of Receipt form will be filed with the individual's record.

6. If the individual first receives services via telehealth and the Notice is sent via email or USPS mail this will be documented in the record by staff.
7. A copy of the Notice shall be posted in clear and prominent locations where it is reasonable to expect clients to be able to read it. Additionally, the Notice will be posted and available electronically on the County web site.
8. The County may revise its Notice of Privacy Practices from time to time to reflect changes in the law or to reflect its own updated operational needs.

B. Right to Request Special Privacy Protections for PHI (45 CFR 164.522(a))

1. The County HIPAA Privacy Officer, and when appropriate, the HIPAA Compliance Committee, shall consider a client's request for a restriction on the use or disclosure of their PHI for treatment, payment or healthcare operations purposes or for restrictions on disclosures otherwise permitted in certain circumstances such as disclosures to a person directly involved in the individual's care or payment for their care or to notify a family member that the individual is deceased.

2. The County is not required to agree to a restriction unless the request is to restrict disclosure to a health plan and the disclosure is related to payment or operations purposes, is not otherwise required by law, and the disclosure pertains solely to a health care item or service for which the individual or other person on behalf of the individual has paid the County in full.

3. If the County agrees to a special privacy restriction it will document the restriction and retain such documentation for at least six (6) years.

4. If the County agrees to a requested restriction it will not use or disclose the individual's PHI in violation of the restriction unless the individual is in need of emergency treatment and the restricted PHI is needed to provide that treatment; the information may then be used or disclosed to a health care provider to provide emergency treatment to the individual.

5. If the County agrees to a restriction for something other than treatment, payment or operations, it shall not be effective if the information is permitted or required to be disclosed in an emergency, or otherwise is permitted or required under law without the need for authorization.

6. Requests for restrictions must be made in writing and the Request for Special Privacy Measures form (Appendix 6) should be used; if the form is not available the written request should include the following specific information:
   a. What information to limit;
   b. Whether the limitation is for use, disclosure, or both; and
   c. To whom the limitation applies (e.g., disclosure to a spouse).

7. An agreement to a special restriction may be terminated as follows:
   a. If the individual requests the termination, or is notified by the County and agrees to the termination in writing;
   b. If the client verbally requests or agrees to the termination and the verbal request or agreement is documented; or
   c. If the County informs the client that it is terminating the restriction; however, the termination shall be effective only with respect to PHI created or received after the client has been notified of the termination.

C. Request for Alternative Means or Location of Confidential Communications (45 CFR 164.522(b))

1. Individuals shall have the right to request alternative means or alternative locations for receipt of confidential communications from the County.
2. The County will accommodate reasonable requests by individuals to receive communications of PHI by alternative means or at alternative locations. For example, an individual may not want their appointment reminders or bills sent to their home address where family members may see them, or they may prefer that email be used for all communications.
3. Requests should be in writing and should use the County Request for Alternative Communication form (Appendix 7). All documented requests and accommodations agreed to by the County shall be maintained for at least six (6) years, and appropriate notation made in the record so that employees who use or access the PHI are aware of the request and the County's accommodation of the request.
4. The County shall not require an explanation from the individual as to why the request for alternative means or location of communication is being made.
5. The County may condition the provision of a reasonable accommodation on the receipt of information from the individual on how payment, if any, will be handled and specification of an alternative address or other method of contact for payment purposes.

D. Access to PHI (45 CFR 164.524; California Health & Safety Code 123100 et seq.)

1. Individuals have a right to inspect and obtain a copy of their PHI that is in a designated record set for as long as the information is maintained by the County, including both medical and billing information, but excluding "psychotherapy" notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
   a. "Designated record set" means the group of records maintained by or for the County and records that are used in whole or in part to make decisions about the individual.

   b. "Record" includes any item, collection or group of information that includes PHI and is maintained, collected, used or disseminated by or for the County.

   c. "Psychotherapy notes" are defined in the law as the private notes maintained by a mental health care professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. The definition of psychotherapy notes specifically excludes information that is considered part of the designated record set: medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

   d. Individuals have a right to access PHI created by another provider that is maintained by the County and included in the designated record set and referred to in making decisions about the individual's care.

2. Access to an individual's record and PHI may be denied without the opportunity for review in the following circumstances:
   a. The PHI falls within the definition of "psychotherapy notes" and is maintained separately from the designed record set or has been prepared in anticipation of, or for use in, a civil, criminal or administrative matter as described in section D. 1. above.

   b. The person making the request is an inmate in the jail or is in the juvenile hall and access would jeopardize the health, safety, security, custody, or rehabilitation of the individual

or others, or the safety of any officer, employee, or other person at the correctional care facility or responsible for the transport of the individual (e.g., taking the individual to a medical appointment).

c. The requested access involves PHI created or obtained by the County in the course of research that includes treatment where access may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the individual has been informed that the right of access will be reinstated upon completion of the research.

d. The requested access is to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, where access may be denied if under the Privacy Act the denial would meet the requirements of that law.

e. An individual's request for access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

3. Access may be denied to an individual in the following circumstances, with a right to have the denial reviewed:
   a. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

   b. The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

   c. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

4. If access is requested to a minor’s PHI and the individual making the request for access is

the parent or legal guardian, described under HIPAA as the "personal representative" of the minor Consumer, access must be denied if the minor, pursuant to California minor consent laws could have, or in fact did consent to the care or treatment reflected in the records and therefore has the right to access that PHI; the minor may choose to execute an authorization to disclose information to the parent/legal guardian in order for the PHI to be disclosed in those cases.

5. If access is requested to a minor's PHI where the minor Consumer would not have a right to consent to the care under California minor consent laws, the parent or legal guardian may be denied access if the health care provider determines that access to the Consumer records requested by the personal representative of the minor would have a detrimental effect on the provider's professional relationship with the minor Consumer or the minor's physical safety or psychological well-being. The decision of the health care provider as to whether or not a minor's records are available for inspection or copying would not attach any liability to the provider under California law, unless the decision is found to be in bad faith.

6. The County shall determine within a reasonable time whether or not to deny the request for access; if access is denied pursuant to paragraph (3) above, the individual shall be notified of the denial within a reasonable time and will be told of their right to have the denial reviewed.

7. If the individual requests a review of the decision, the denial will be promptly referred for a review to a licensed healthcare professional who did not participate in the original decision to deny and who is designated by the County to act as the reviewing official; the designated reviewing official shall determine within a reasonable period of time whether or not to deny the access requested.

8. Written notice will be promptly provided to the individual of the determination of the designated reviewing official, and action will be taken as necessary to carry out the reviewing official's decision. The reviewing official shall make the final decision on whether access will be provided or denied in the situations described in paragraph (3).

9. If the individual is seeking access to their mental health records, and that access has been denied pursuant to paragraph (3) with the right to review, and the denial has been supported by a reviewing official's determination pursuant to paragraph (6), the individual has a right under California law to request the County to permit inspection on the individual's behalf by, or to provide copies of the mental health records to, a licensed

physician and surgeon, licensed psychologist, licensed marriage and family therapist, licensed clinical social worker, or licensed professional clinical counselor, designated by request of the Consumer.

a. Any person registered as a marriage and family therapist intern, as defined in Chapter 13 (commencing with Section 4980) of Division 2 of the California Business and Professions Code, may not inspect the Consumer's mental health records or obtain copies thereof, except pursuant to the direction or supervision of a licensed professional specified in subdivision (g) of Section 4980.03 of the Business and Professions Code. Prior to providing copies of mental health records to a registered marriage and family therapist intern, a receipt for those records shall be signed by the supervising licensed professional.

b. Any person registered as a clinical counselor intern, as defined in Chapter 16 (commencing with Section 4999.10) of Division 2 of the California Business and Professions Code, may not inspect the Consumer's mental health records or obtain copies thereof, except pursuant to the direction or supervision of a licensed professional specified in subdivision (h) of Section 4999.12 of the Business and Professions Code. Prior to providing copies of mental health records to a person registered as a clinical counselor intern, a receipt for those records shall be signed by the supervising licensed professional.

c. A licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, licensed clinical social worker, licensed professional clinical counselor, registered marriage and family therapist intern, or person registered as a clinical counselor intern to whom the records are provided for inspection or copying shall not permit inspection or copying by the Consumer.

d. The original health care provider shall inform the Consumer of the right to require the County to permit inspection by, or provide copies to, a licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, licensed clinical social worker, or licensed professional clinical counselor designated by written authorization of the Consumer.

e. The original health care provider shall indicate in the mental health records of the Consumer whether a request was made for independent review of the PHI by a licensed health care professional selected by the individual.

f. The health care provider shall make a written record, to be included with the mental health records requested, noting the date of the request and explaining the health care provider's reason for refusing to permit inspection or provide copies of the records, including a description of the specific adverse or detrimental consequences to the Consumer that the provider anticipates would occur if inspection or copying were permitted.

10. The County shall document its description of the "designated record sets" it maintains that are subject to access by individuals, the titles of persons or offices responsible for receiving and processing requests for access, and any denials of access; in the case of denials based upon reasons listed in paragraph (3) that trigger a right to review, documentation will indicate whether a review was requested, and if requested by the individual, documentation will include the recommendations, reasons and conclusions of the reviewing official for those recommendations.

11. Documentation related to requests for access to individuals' health records will be maintained for a minimum of six (6) years.

12. Individuals may request access to their PHI in writing using the form developed by the County (see Appendix 2) or by any other means that is clear, conspicuous and specific.

13. The County will not require that an individual submit their request in person, nor will the County impose any other measures on an individual, whether the individual is the Consumer or the Consumer representative, that would create barriers to access, or unreasonably delay the individual from obtaining access. Any requirements related to requesting access shall not be used oppressively or discriminatorily to frustrate or delay compliance with the request.

14. County employees may make reasonable efforts to verify an individual's identity, for example by comparing the signature on a written request to a signature already on file with the PHI.

15. When verbal requests are made by telephone, and a written request would unduly delay the process, County employees may ask for verifying information from the caller, for example, name, date of birth, name of provider and approximate date of last visit or reason for last visit.

16. County staff may also make inquiries related to an individual's request for medical information to seek clarity about the exact information or documents that the client seeks.

17. Access to the PHI by inspection shall be permitted during business hours within 5 working days after receipt of the request, as provided by California law.

18. The individual shall be entitled to a paper or electronic copy of the PHI that an individual is permitted to inspect upon presenting a request specifying the records to be copied, together with a fee to defray the costs of producing the copy; the copy shall be transmitted within 15 calendar days of the request in a form or format requested if it is readily producible in the requested form and format, or, if not, in a readable paper copy form or other form and format as agreed to by the individual and the County.

19. The fee charged to the individual for the copy of the record shall be a cost-based fee that under no circumstances exceeds 25¢/page or 50¢/page for copies made from microfilm.
    a. Special rules apply to copies of x-rays or other tracings and those requests should be referred to the HIM (HHSA) Manager.

        i) In any case where the amount charged exceeds $6.50, the provider should be prepared to produce documentation and receipts to a surveyor that demonstrate the cost-basis for the fee charged.

        ii) The fee charged may only include the cost of the following: labor for copying the Consumer records requested by the Consumer or Consumer's personal representative, whether in paper or electronic form; supplies for creating the paper copy or electronic media if the Consumer or Consumer's personal representative requests that the electronic copy be provided on portable media; postage, if the Consumer or Consumer's personal representative has requested the copy, or the summary or explanation, be mailed; and, reimbursement for the time taken to prepare an explanation or summary of the Consumer record, if agreed to by the Consumer or Consumer's personal representative. Costs associated with locating the record cannot be passed along to the individual.

    b. An individual Consumer, employee of a nonprofit legal services entity representing the Consumer, or the personal representative of a Consumer, is entitled to a copy, at no charge, of the relevant portion of the Consumer's records, upon presenting to the provider a written request, and proof that the records or supporting forms are needed

to support a claim or appeal regarding eligibility for a public benefit program, a petition for U nonimmigrant status under the Victims of Trafficking and Violence Protection Act, or a self-petition for lawful permanent residency under the Violence Against Women Act. A public benefit program includes the Medi-Cal program, the In-Home Supportive Services Program, the California Work Opportunity and Responsibility to Kids (CalWORKs) program, Social Security Disability Insurance benefits, Supplemental Security Income/State Supplementary Program for the Aged, Blind and Disabled (SSI/SSP) benefits, federal veterans service-connected compensation and nonservice connected pension disability benefits, CalFresh, the Cash Assistance Program for Aged, Blind, and Disabled Legal Immigrants, and a government-funded housing subsidy or tenant-based housing assistance program.

c. Although a Consumer shall not be limited to a single request, the Consumer, employee of a nonprofit legal services entity representing the Consumer, or Consumer's personal representative shall be entitled to no more than one copy of any relevant portion of their record free of charge.

d. Subsection (b) and (c) shall not apply to any Consumer who is represented by a private attorney who is paying for the costs related to the Consumer's claim or appeal, pending the outcome of that claim or appeal. For purposes of this subdivision, "private attorney" means any attorney not employed by a nonprofit legal services entity.

e. If a Consumer, employee of a nonprofit legal services entity representing the Consumer, or the Consumer's personal representative requests a record pursuant to subdivision (b) or (c), the health care provider shall ensure that the copies are transmitted within 30 days after receiving the written request.

f. If a Consumer or personal representative requests that a copy of their PHI be provided to their attorney before the filing of any action or the appearance of a defendant in an action, pursuant to California Evidence Code section 1158 of the Evidence Code the fee charged may not exceed 10¢/page for standard reproduction of documents of a size 8 ½ by 14 inches or less, and 20¢/page for copying of documents from microfilm. If oversize documents or reproduction of documents requiring special processing, reasonable clerical costs can be billed at a maximum rate of sixteen dollars ($16) per hour per person, computed on the basis of four dollars ($4) per quarter hour or fraction thereof; actual postage charges; and actual costs, if any, charged to the witness by a third person for retrieval and return of records held by that third person.

20. If an individual requests a summary instead of a copy of the actual record, a summary may be provided at the discretion of the healthcare professional, but County staff shall not insist that a summary be provided in lieu of providing access or a copy of the record.

E. Right to Request an Amendment to PHI [45 CFR 164.526]

1. Individuals shall have the right to request an amendment to their PHI for as long as such PHI is maintained by the County.

2. Requests for amendments should be submitted in writing using the Request to Amend Health Record form (Appendix 4) and provide a reason that supports the request.

3. Amendments may be denied under the following circumstances:
   a. The information being requested for amendment is accurate and complete;

   b. The PHI was not created by County;

   c. The information at issue is not part of the medical information kept by the County; or

   d. The information is not part of the PHI that the client would be permitted to access and obtain a copy.

4. If a request to amend PHI is denied, the Privacy Officer shall be notified and will review the request and denial to ensure that all statutory procedures are followed.

5. If there will be a denial of the request, the individual shall be notified of the denial and of the reason(s) for denying the request. The notification to the individual shall contain:
   a. The basis for the denial;

   b. A description of the individual's right to submit a written statement disagreeing with the denial, and how to file the statement;

   c. A statement that, if the individual does not submit a statement of disagreement, the individual may request that the County include a copy of the request for amendment and the denial in any future disclosures; and,

d. Instructions on how the client may complain to the County pursuant to its complaint procedures outlined in Part 1 of the Privacy and Protected Information Policy (Administration) or to the Secretary of the US Department of Health and Human Service.

6. If a request to amend PHI is denied, the client shall have the right to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement; the County may then prepare a written rebuttal to the individual's statement of disagreement and provide a copy to the individual.

7. The request, denial letter, individual's statement of disagreement and the County's rebuttal shall be attached to the individual's records and included whenever County makes a disclosure of the item or the record that the client believes to be incomplete or incorrect.

F. Right to Addendum/Add to the Record

1. Individuals have a right under California state law to add an addendum to their record of up to 250 words.

2. An individual must make the request to add an addendum to the record in writing and should use the County's "Request to Addend/Add To the Record" form (Appendix 11).

3. If an addendum is submitted, it shall be added to the individual's record as requested and included in all future disclosures of the record; the County is not required to comment on the addendum and does not have the responsibility under state law to approve it, or the authority to deny it.

G. Right to an Accounting of Disclosures (45 CFR 164.528, W&I Code 5328.6)

1. The County shall respond in writing to any client requests for an accounting of how their PHI has been disclosed. Such response and accounting shall include:
   a. A list of disclosures for the six (6) years prior to the request, unless the client wants information for a shorter time period;

   b. Disclosures made to or by business associates;

   c. The date of each disclosure;

d. The name of the person or entity who received the PHI, including an address if possible;

e. A brief description of the information disclosed; and

f. A brief statement of the purpose of the disclosure.

2. Accountings do not need to include disclosures made for the following purposes:
   a. For treatment, payment or the County's own health care operations;

   b. To clients regarding their own information;

   c. Pursuant to an authorization signed by the client or their authorized representative;

   d. To persons involved in the client's care when there has been verbal permission;

   e. For notification purposes (e.g. to notify a family member, personal representative or other person of the client's location, general condition or death);

   f. Incident to use or disclosures otherwise permitted by HIPAA;

   g. For certain national security or intelligence purposes;

   h. To correctional facilities or law enforcement officials working with correctional institutions; or,

   i. As part of a limited data set

3. If during the period covered by the accounting, the covered entity has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may with respect to multiple disclosures include the information for the first disclosure as required by this policy, and then simply include the frequency, periodicity or number of disclosures made during the accounting period, and the date of the last such disclosure during the accounting period.

4. If disclosures have been made for a particular research purpose involving the PHI for 50 or more individuals, the accounting may, with respect to the PHI of the individual that may have been included provide the name of the protocol or research activity, a description in plain language of the type of PHI that was disclosed, the date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period, the name, address and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed, and a statement that the PHI of the individual may, or may not have been disclosed for a particular protocol or other research activity.

5. individuals will be provided an accounting no later than 60 days after submitting their request for an accounting; such time may be extended by no more than 30 days if the County is unable to provide an accounting within 60 days, but only if it provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting.

6. Clients will be provided the first accounting of disclosures free of charge. A reasonable, cost-based fee may be charged for each subsequent request for an accounting within the same 12-month period as long as the client has been informed in advance of the fee and the client has had the opportunity to withdraw or modify the request.

7. The County shall document the following and retain the documentation for a minimum of six (6) years after the accounting has been requested: a copy of the accounting provided to the individual including any delay and reason for the delay in providing the accounting, and any statements regarding the delay that were made to the individual, and the titles of the persons or offices responsible for receiving and processing request for an accounting.

H. Right to Submit a Complaint if a Client Believes PHI has been Improperly Used or Disclosed.

1. Clients may submit a complaint to the HIPAA Privacy Officer or HIPAA Compliance Committee if they believe their PHI has been improperly used or disclosed. They may also submit a complaint to the Secretary of the US DHHS. (See County Privacy and Protected Information Policy, Part 1 -- Administration, describing the Complaint Process.) The complaint may be submitted orally, but may also be submitted on the County HIPAA Complaint Form (Appendix 1).
2. County employees shall assist any individual who needs assistance filling out the HIPAA

Complaint Form.

3. All complaints should be forwarded to the HIPAA Privacy Officer who will review all complaints; all serious complaints will be referred to the HIPAA Compliance Committee for direction and investigation.
4. The HIPAA Privacy Officer shall log all complaints including those related to the County's handling of an individual's PHI, improper use or disclosure of PHI, the exercise of Consumers' rights regarding their PHI, or security issues or alleged breaches, and shall maintain the log and complaints, as well as information related to investigations for no less than six (6) years.
5. Anyone who files a complaint or requests information on how to file a complaint shall not be retaliated against or denied any services or rights, whether the complaint is made by a Consumer, client, consumer, employee or some other person.
6. Anonymous complaints may be made by anyone at any time and will be investigated to the extent possible if they raise serious concerns.

I. Right to be Notified in the Case of Breach (45 CFR 164.404)

1. The County HIPAA Privacy Officer, or HIPAA Compliance Committee shall notify any individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of a reportable breach. (See County Privacy and Protected Information Policy, Part 5 - Breaches for additional details about the content and timing of the notification.)
2. The County HIPAA Privacy Officer, or HIPAA Compliance Committee shall have the sole responsibility for notifying individuals of a breach, reporting the breach to appropriate state and federal agencies, overseeing mitigation efforts, and making recommendations regarding sanctions to the appropriate County human resources staff. These responsibilities may be delegated as necessary and appropriate. No other County employee shall contact an individual regarding a breach without direction from the HIPAA Privacy Officer or HIPAA Compliance Committee.

4.3 REFERENCES

45 CFR Part 160, Subpart D (Sections 45 CFR 164.400 - 164.414)

California Health and Safety Code, sections 123100 - 123149.5 (PAHRA)

5.0 Breach Reporting

5.1 PURPOSE

A. The purpose of this policy is to provide guidance to staff regarding the requirements to notify individuals (clients and consumers) of privacy/security breaches of protected health information (PHI) protected by the Health Insurance Portability and Accountability Act (HIPAA), and to report those breaches to the Secretary of the Department of Health and Human Services (DHHS) as mandated by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Title XIII of Division A of the American Reinvestment and Recovery Act of 2009 (ARRA) and the regulations found in the Final Rule published January 25, 2013 in the Federal Register (78 Fed. Reg.5566) and found in 45 CFR Part 164, Subpart D. (See below for definition of what a reportable breach is at III. A.)

B. Additionally, this policy reiterates the requirement that HIPAA breach response obligations include mitigation of harm and sanctioning of the employee(s) responsible for the breach or who failed to follow County of El Dorado (County) HIPAA policies and procedures.

C. This policy also addresses the reporting of breaches of computerized data to the California residents, and in the case of large breaches to the Attorney General; the reporting of breaches in a licensed healthcare facilities to the individual and to the California Department of Public Health (22 CCR 7990-79905), and in the case of Medi-Cal Consumers, to the California Department of Health Care Services.

5.2 POLICY

A. It shall be the policy of the County of El Dorado to actively encourage the reporting of suspected or known privacy breaches or concerns by Consumers, members of the workforce, or others, and to promptly investigate any reports.

B. If the investigation shows that a breach did indeed occur, steps will be taken to a) mitigate harm to the Consumer, b) sanction the employee(s) if there was a violation of the law or of County policy and procedure, c) notify the Consumer of the breach, and d) report the breach to appropriate governmental agencies and the media in the case of a large breach, as required by federal and state law, or as required under contractual relationships with health plans.

5.3 DEFINITIONS

The following definitions shall apply:

A. **"Breach"** is defined as the acquisition, access, use, or disclosure of "unsecured" PHI in a manner not permitted by the (HIPAA) Privacy Rule which compromises the security or privacy of the PHI. Breach also means the unlawful or unauthorized access to, or use or disclosure of, a Consumer's medical information. "Unauthorized" means the inappropriate access, review, or viewing of medical information without a direct need for medical diagnosis, treatment or other lawful use under any state or federal law.

B. **"Compromises the security or privacy"** means that an acquisition, access, use or disclosure of protected health information that occurred in a manner not permitted by the HIPAA Privacy Rule will be presumed to be a breach unless the Covered Entity (or Business Associate), demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. nature and extent of PHI involved, including types of identifiers and likelihood of re-identification;

2. the unauthorized person who used the PHI or to whom the disclosure was made;

3. whether the PHI was actually acquired or viewed;

4. the extent to which the risk to the PHI has been mitigated.

C. **"Unsecured Protected Health Information**" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of DHHS in the guidance under section 13402(h)(2) of Pub.L. 111-5.

D. **Exceptions: the term "breach" does NOT include**:

1. Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate if the acquisition, access or use was made in good faith and within the course and scope of the authority and does not result in further use or disclosure in a manner not permitted by the HIPAA.

2. Any inadvertent disclosure by a person who is authorized to access PHI at the County or one of its business associates to another person authorized to access PHI at the County or its business associate, or organized health care arrangement (OHCA) in

which the County participates, and the information received is not further used or disclosed in a manner not permitted by HIPAA.

3. A disclosure of PHI where the County or its business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information, for example, sending PHI in the mail to the wrong address where the mail is returned unopened to the post office as undeliverable, or where a healthcare provider mistakenly hands discharge paperwork to the wrong Consumer, quickly realizes the mistake, and recovers the PHI before the Consumer has time to read it.

5.4. PROTOCOLS

A. Discovery and Initial Report of Actual or Potential Breach or Violation of County Policy

1. All workforce members of the County, including any employee, volunteer, student, agent, contractor, business associate or other person or entity working on behalf of the County, who becomes aware of or suspects any unauthorized access, use or disclosure of PHI, or a breach in the security of a computerized system containing such information, or any other actual or possible violation of the County HIPAA policies and procedures shall be responsible for immediately reporting such unauthorized access or breach to their supervisor, manager, HIPAA Privacy Officer, or to a member of the HIPAA Compliance Committee. The County is required to report certain violations to the California Department of Health Care Services immediately, if it includes Medi-Cal PII provided or verified by SSA, and within one working day of discovery if it does not include Medi-Cal PII provided or verified by SSA. As such, immediate reporting is essential to meet this required timeline. The violation must be reported whether committed by the person reporting the violation, or another individual and it must be reported whether intentional or accidental.

2. Initially, workforce members may contact their supervisor, department privacy officer, HIPAA Privacy Officer, or a member of the HIPAA Compliance Committee by phone. Following any initial verbal report, an electronic submission of the HIPAA Complaint Form shall always be filled out and submitted within four (4) business hours of discovery of the problem.

3. In addition to the above, workforce members may choose to file HIPAA complaints or report violations directly via the U.S. Department of Health and Human Services (hhs.gov) Health Information Privacy website at https://www.hhs.gov/hipaa/filing-a-

complaint/index.html or in writing to Centralized Case Management Operations, U.S. Department of Health and Human Services, 200 Independence Avenue, S.W., Room 509F HHH Bldg., Washington, D.C. 20201, or by email to OCRComplaint@hhs.gov.

B. **Investigation of Potential or Actual Breach**

1. The HIPAA Compliance Committee is responsible for facilitating a response in support of the appropriate workforce members of the division, unit or program that reported the suspected or actual breach. Each workforce member is required to cooperate with the HIPAA Compliance Committee in identifying what information was inappropriately accessed, used, disclosed, compromised, misplaced or stolen.

2. An assessment will be done and documented in the case of every potential reportable breach to determine whether it meets one of the three exceptions listed in the definitions section of this policy, or that based upon a risk assessment, it is determined that there is a low probability that the PHI has been compromised. The assessment will include a determination whether the breach involved computerized data and is also reportable per California Civil Code section 1798.82, or whether it triggers any contractual obligations related to notifying health plan enrollees and reporting to the plan, for example, the Medi-Cal program and reporting duties to the California Department of Health Care Services.

3. If a reportable breach occurred, the HIPAA Compliance Committee in cooperation with the reporting division or program, shall be responsible for the management of the breach investigation, including conducting interviews, risk assessments, and coordinating with other county departments as appropriate (e.g., Information Security Officer, Human Resources, Risk Management, and the Office of County Counsel).

4. Examples of unauthorized activities that will be investigated include but are not limited to, the following:

    a. Accessing their own PHI without following the proper access protocol, or accessing the protected health information of a co-worker, colleague, friend, family member, or client without authorization or business necessity as allowed by law;

    b. Accessing the PHI of a client without a treatment, payment or administrative purpose or in violation of the minimum necessary rule;

c. Accessing PHI in violation of specific restrictions placed on the information by an individual program or special rules related to a service within the County;

d. Sending faxes, emails or regular mail containing PHI to an unauthorized recipient or in an unsecured manner;

e. Disclosing PHI through any means to those who have no business necessity for the information or who are otherwise precluded from such information without the explicit authorization of the client;

f. Posting any type of PHI or characteristic that could lead to the identification of a Consumer on public websites, social media or any other means of communication;

g. Discarding electronic devices or storage medium without removing all electronic protected health information (ePHI) in a manner prescribed by the County HIPAA Security Officer or in County HIPAA security protocols;

h. Leaving documents containing protected health information in plain view of non-authorized individuals, or in public locations;

i. Lost or stolen access devices, for example swipe card, keys, etc. or the posting or loss of a password or a password list; or

j. Loss or theft of any device containing PHI, or of protected health information in written, electronic or storage medium.

5. In assessing any actual or potential unauthorized activity, the HIPAA Compliance Committee, in cooperation with the reporting division, shall:

a. Determine whether the potential breach fits within one of the following exceptions to the definition of privacy incident and maintain a record of the completed investigation, regardless of whether or not it is determined that there was a breach;

b. Determine whether and what mitigation efforts should be undertaken and oversee such efforts;

c. Determine whether and when sanctions against the involved employee(s) is required and oversee such sanctions;

d. Determine whether and when reporting to the US DHHS and other state agencies is required and oversee such reporting;

e. Determine whether and when notice to the Consumer is required and oversee the provision of such notice if required; and,

f. Determine whether and when notice in the media is required and oversee such notice.

6. All documentation related to the breach investigation, including the risk assessment, shall be retained by the HIPAA Compliance Committee for a minimum of six (6) years unless the breach involves a Medi-Cal Consumer, in which case the records should be kept for a minimum of ten (10) years from the date of service, end of contract period, or audit completion whichever is later (22 CCR 51476; WIC 14124.1).

C. Mitigation - The HIPAA Compliance Committee shall ensure that all steps are promptly taken to mitigate any harmful effects of the breach, and to ensure that all appropriate changes are made to prevent further similar breaches. Mitigation should include provision of identity theft protection if names, dates of birth and social security numbers were breached.

D. Sanctions

1. Employee negligence, carelessness, or repetitive or willful violations of County HIPAA policies and procedures will result in disciplinary action including and up to termination of employment as outlined in the County of El Dorado Personnel Rules.

2. An agent, volunteer or contractor of the County Health Agency who violates any provision of the County HIPAA policies and procedures shall be subject to sanctions which may include but are not limited to contract cancellation or termination of services.

3. Retaliation against any person who in good faith reports a violation of the County's HIPAA policies and procedures, or retaliation against any person who supports someone else who reports a violation of Count policies and procedures, is prohibited. In addition, retaliation against any person who cooperates in any related investigation is prohibited.

E. Consumer or Authorized Representative Notification

1. Timing

   a. State and federal laws require prompt notification without unreasonable delay of any breach to the individual whose information is involved in the breach.

   b. BAA agreements - if the County functions as a BA for another covered entity (e.g., you do billing for one of your healthcare providers), your BA agreement may require you to report a breach to the covered entity within "x" number of days or hours.

   c. California state healthcare facility licensing laws, CA Health and Safety Code §1280.15, require the prompt notification of certain unlawful or unauthorized access to, use or disclosure of Consumers' information not later than 15 business days after the detection of the unlawful or unauthorized access, use or disclosure; additionally certain contractual relationships may also require Consumer notification.

   d. Regardless of licensure, HIPAA - 45 CFR 164.400 et seq., requires breach notification to the Consumer without unreasonable delay and in no case later than 60 days after discovery of the breach unless a delay as described in subsection (d) is requested.

   e. Notification may be delayed if a law enforcement agency or official provides a written or oral statement that notifying the client would likely impede the enforcement agency's investigation of the breach and specifies a date upon which the delay will end, not to exceed 60 days for a written request or 30 days after an oral request is made. A law enforcement agency may request an extension of a delay not to exceed 60 days after the end of the original delay upon declaration of an ongoing criminal investigation of serious wrongdoing.

2. Method

   a. Notice to individual(s) shall be provided in writing by first-class mail to the last known address or by email if the individual has indicated a preference to receive email communication.

b. If notification is urgent because of possible imminent misuse of the unsecured PHI, the individual should be notified by phone or other means as appropriate; additionally, written notification is still required.

c. If the individual is a minor or otherwise lacks capacity due to a physical or mental condition, notice to the parent or personal representative of the client is required.

d. For individuals who are deceased and for whom the County has sufficient contact information for the decedent's personal representative then this individual must be notified in writing through first class mail.

e. For limited English proficiency clientele, notice must be translated appropriately. For those individuals reliant on alternative communication methods i.e., Braille, audio, large print, etc., appropriate accommodation must be made.

f. Substitute Notice

i. Fewer than 10 - If fewer than ten Consumers cannot be reached by first class mail, then substituted means of communication should be employed. This may involve phone calls, website notification, or use of the media, whichever is most likely to reach the individuals.

ii. 10 or more Consumers - If contact information is insufficient or out of date precluding written notification, and 10 or more Consumers cannot be reached, then one of the following is required: a) a conspicuous posting on the County's home page of their website, OR b) notice in major print or broadcast media (including major media where individuals likely reside). Either method requires a minimum posting of 90 days and a toll-free number (active for at least 90 days) that an individual can call to find out if his/her unsecured PHI was included in the breach.

3. Content - the content of notice to client must use plain language and be translated as may be required by other applicable laws; the notice must include the following information:

a. Brief description of what happened, including the date of breach and date of discovery of breach, if known;

b. Description of types of unsecured PHI involved (such as whether full name, SSN, date of birth, home address, account number, diagnosis, disability code, etc.);

c. Steps clients should take to protect themselves from potential harm including, if computerized data was breached, the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a SSN or driver's license or California ID number; additionally, information regarding identity theft prevention services should be included if offered as a part of mitigation of the breach;

d. Brief description of what the County is doing to investigate, mitigate, and protect against further breaches; and,

e. Contact information for Consumers to obtain further information, including toll-free phone number, email address, website address, or street address.

F. Reporting to Secretary of the Department of Health and Human Services (DHHS), California State Attorney General, California State Department of Public Health (Licensing) and California Department of Health Care Services (Medi-Cal), as appropriate.

1. The HIPAA Compliance Committee, including the County Privacy Officer and/or County Security Officer, shall facilitate all breach reporting processes to the appropriate entities as required.

2. Special reporting circumstances unique to specific types of breaches or locations of the breach will be governed by specific program guidance, mandates, state or federal direction, and contractual obligations, and will be coordinated by the HIPAA Compliance Committee in collaboration with assigned departmental workforce members; this may include reporting to the United States Department of Health and Human Services ("HHS"), the California Attorney General if computerized data of more than 500 individuals is breached, Department of Public Health ("CDPH") if the breach occurs in a licensed healthcare facility (e.g., a PHF or licensed clinic), California Department of Health Care Services ("DHCS") if the breach involves Medi-Cal Consumers' information (Medi-Cal Personally Identifiable Information or "PII"), or to some other individual or entity as a result of other contractual obligations.

3. The HIPAA Compliance Committee shall provide information regarding the appropriate notification process for each privacy event.

4. Timing

   a. If fewer than 500 individuals were affected, breach reports may be submitted to DHHS via an annual log no later than 60 days after the end of each calendar year (i.e., by March 1 or Feb 29 in leap years).

   b. If 500 or more individuals were affected, HIPAA breaches must be reported at the same time that individuals are given notification of the breach.

   c. In the case of a breach of computerized data, the report should be submitted to the Attorney General in the most expedient time possible and without unreasonable delay.

   d. In the case of a licensed facility breach, the report should be made to CDPH no later than 15 days after detection unless there is a law enforcement request for a delay.

   e. In the case of Medi-Cal PII breaches, the report should be made immediately if SSA information is involved and within one working day of discovery otherwise.

5. Method
   a. Reports of all HIPAA breaches should be made directly to the US Health and Human Services Agency via the U.S. Department of Health and Human Services (hhs.gov) Health Information Privacy website at https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

   b. The reporting to California Department of Public Health (CDPH) that is triggered if the breach occurred in a *licensed* facility is required within 15 business days after detection and should be made to the CDPH via the web portal on the Online California Healthcare Event and Reporting Tool (CalHEART) website at https://healthcareportal.cdph.ca.gov.

   c. Reporting of computerized data breaches should be made to the State Attorney General; see oag.ca.gov/ecrime/databreach/report-a-breach.

G. Notification of the Media - The media must be notified of a HIPAA breach if more than 500 residents of a State or jurisdiction are affected.

1. Timing - The media notification must be made without unreasonable delay, but in no case later than 60 calendar days after discovery, unless a law enforcement delay has been requested and this exception applies (see subsection E 1.c. above).

2. Method - The County will provide this notification to the media in the form of a press release to appropriate media outlets serving the area. The press release verbiage should be drafted or reviewed by the HIPAA Privacy Office and/or the HIPAA Compliance Committee prior to publication.

3. Content - The content of notice to media, like the notice to the individual, must be in plain language, and if appropriate be translated, and include the following information:

   i. Brief description of what happened, including the date of breach and date of discovery of breach, if known;

   ii. Description of types of unsecured PHI involved (such as whether full name, SSN, date of birth, home address, account number, diagnosis, disability code, etc.);

   iii. Steps clients should take to protect themselves from potential harm;

   iv. Brief description of what the County is doing to investigate, mitigate, and protect against further breaches; and,

   v. Contact information for Consumers to obtain further information, including toll-free phone number, email address, website address, or street address.

H. Notification of a Breach by a Business Associate (BA)

1. Assigned County workforce members in cooperation with the HIPAA Compliance Committee and a representative from the El Dorado Office of County Counsel will coordinate with the Business Associate (BA) to ensure that the County receives prompt notification of any breach and any related information and documentation in accordance with the privacy terms of the applicable Business Associate Agreement.

2. The business associate must provide notice to the County without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the County with the identification of each individual

affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.

I. Accounting of Disclosures

1. All breaches must be logged in such a manner that if an affected individual or their personal representative requests an accounting of disclosures at any future date, the County will be able to disclose the breach on the accounting. The HIPAA Compliance Committee shall determine the means and mechanism for maintaining and archiving disclosure logs involving breach situations.

2. The HIPAA Compliance Committee shall determine (with specific guidance from the individual representing County Counsel) whether unauthorized activity is subject to inclusion for disclosure on the individual audit of disclosures based on the event circumstances.

J. Post-Investigation Follow-Up and Closing

1. The HIPAA Compliance Committee will work as necessary to continue to mitigate any harmful effects of any breach that is known to the County regardless of whether it was due to the County's conduct or a business associate's conduct.

2. When necessary, a change in policy or additional education will be provided to the department or facility staff involved in the breach event.

5.5. REFERENCES

HIPAA, 45 CFR Part 164, Subpart D
California Health & Safety Code 1280.15
California Civil Code 1798.28; 1798.82
Medi-Cal Privacy & Security Agreement No. 19-16

V. RESPONSIBLE DEPARTMENT(S)

County Counsel
Health and Human Services Agency
Human Resources
Information Technologies

Subject:	Policy Number:	Page Number:
PRIVACY AND PROTECTED INFORMATION POLICY	L-1	80 of 80
	Originally Adopted: 08/29/2017	Last Revised Date: 03/21/2023

VI. DATES (ADOPTED, REVISED, NEXT REVIEW)

Originally Adopted:	08/29/2017		
Last Revision:	03/21/2023	**Next Review:**	03/21/2026