HIPPAA PHASE II ASSESSMENT

REPORT AND

RECOMMENDATIONS

CONTENTS:

PHASE II SUMMARY

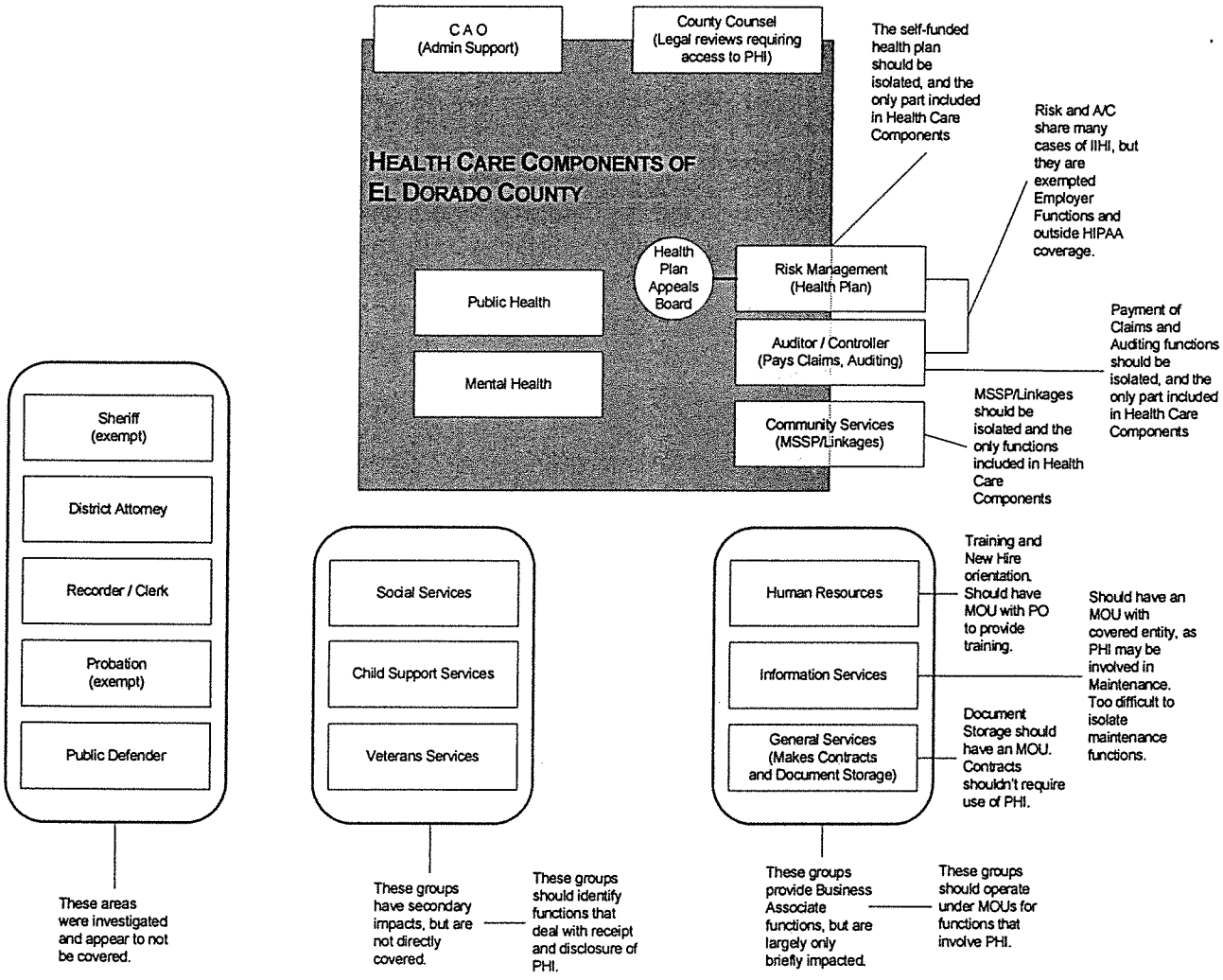
EL DORADO PHASE II: DETAILED HIPAA ANALYSIS

Findings:

I. Organizational Findings:

1. El Dorado County is a Hybrid Entity:
   a) Two departments are completely covered
   b) Three Departments have some covered functions
   c) Two Departments are included for support reasons
   d) Three departments are not covered but provide Business Associate function
   e) All other departments are not covered, but may have secondary or incidental impacts.

Designation of Health Care Components of El Dorado County



2. El Dorado County has not designated a County Privacy Official or Contact Office.
3. El Dorado County has no County-level statement of privacy rights or confidentiality.
4. Some departments do have a confidentiality statement that is signed by employees.

IV. Software and Databases:

The Health Care Components have inventoried all of the databases and software systems they use to create and maintain health information. These lists are being reviewed to determine which systems transmit Protected Health Information using any of the HIPAA identified transactions. In addition, the lists are being reviewed to determine which applications and databases require physical or electronic safeguards because of their location or accessibility.

V. Physical Safeguards:

The Health Care Components have conducted (or are conducting) physical walk-throughs of locations used by each Department. These walk-throughs are being used to determine where records are stored, computers can be accessed, and information can be transmitted (faxes and printers). These walk-throughs will also identify where physical safeguards such as Fire extinguishers, locking file cabinets and limited-access work areas are already in place. Finally, these walk-throughs are used to determine if procedures used affect physical security of the data (passwords written on monitors, clean desk requirements, visitors excluded or escorted, etc.). This data will be used to determine where additional safeguards may be required to ensure the confidentiality of PHI used at each facility.

VI. Security:

From January 27, 2003, through February 7, 2003, the Department of Information Systems will be conducting a HIPAA Security Rule Current State and GAP analysis. The results of this analysis will address the County's Electronic Security and Data Safeguards.

stringent California State Law. Specific training needs cannot be assigned until County Compliance policies are in place.

VII. Policies and Procedures:

1. Create County-wide policies and procedures required to establish county organizational structure and to become compliant with the Final HIPAA Privacy Rules.
2. Review and apply Preemptive State Law to County Privacy Policies and Procedures.
3. Draft/Document department-level policies and procedures to properly implement County Privacy Policy.
4. Draft the County Notice(s) of Privacy Practices.

To comply with the Final HIPAA Privacy Rules, the County will be required to have in place certain written policies and procedures. In addition, the County will be required to comply with any more stringent California State Law (Preemptive State Law). Individual Departments with Health Care Components will be required to have documented Policies and Procedures that ensure they are compliant with County Policy.

The Final HIPAA Privacy Rules require covered entities to provide and follow a Notice of Health Care Information Privacy Practices. As a Hybrid Entity, the county should provide this notice at the highest level of the Hybrid Structure, and allow the covered Health Care Components to add specific statements, if required. All Health Care Components would provide the same notification.

VIII. Contracts, MOUs and other Business Relationships:

1. Create standard legal language to be used for Business Associate contracts and MOUs.
2. Create standard legal language to be used for Authorizations.
3. Review and amend contracts identified by Phase II as Business Associates.
4. Create "Business Associate" MOUs where needed.

To comply with the Final HIPAA Privacy Rules, the County will be required to ensure that all "Business Associates" are bound by a written agreement or contract, and that these agreements have certain required elements. The Phase II inventories uncovered approximately 145 outside agencies that would require contract amendments or the addition of other written agreements. In addition, approximately 18 MOUs would require similar action. To ensure consistency, and speed the processing required to address these agreements, the County should have a standard set of clauses created. In this way, contracts can be amended by selecting the appropriate language for the relationship, rather than separately authoring each amendment.

In a similar fashion, certain disclosures by the County may require written authorization from the patient. In most cases, authorization or consent is already obtained. These written agreements will need to be created or revised to include specific HIPAA required language. A standard format and standard wording would ensure that each of these events is compliant and consistent.

IX. Software and Databases:

1. Collect documentation and compliance information from Business Associates and other suppliers that provide software and access for the transmission of Protected Health Information using standard Transactions, Code Sets, and Identifiers (TCI).
2. Develop plans for the upgrade or replacement of software that uses TCI in the event these systems are not brought into compliance.
3. Develop reasonable safeguards for the protection of software and databases that contain health information.

HIPAA HYBRID ENTITY RECOMMENDATION

EL DORADO PHASE II: DETAILED HIPAA ANALYSIS

Recommendation:

El Dorado County should declare itself a *Hybrid Entity* under the HIPAA Final Privacy regulations and designate those areas that must comply with the HIPAA rules as *Health Care Components*.

Definition:

As defined in the Final Privacy Regulation Sec. 164.504(a):

> ***Hybrid entity*** *means a single legal entity:*
> *(1) That is a covered entity;*
> *(2) Whose business activities include both covered and non-covered functions; and*
> *(3) That designates health care components in accordance with paragraph (c)(3)(iii) of this section.*
>
> ***Health care component*** *means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with paragraph (c)(3)(iii) of this section.*

The County has many activities that would, if considered separately, be considered covered entities or business associates of covered entities.

Justification:

The County has many departments and functions that are covered under the HIPAA regulations, and thus has a responsibility to comply. By approaching compliance to HIPAA from the county level, as a Hybrid Entity, the County will be able to Ensure Compliance, Provide Consistency, Limit the burden of Compliance, and Reduce the Costs of compliance.

Ensure Compliance

By approaching compliance to HIPAA from the county level, as a Hybrid Entity, the County will be able to:

- Ensure that those areas impacted by HIPAA are identified.
- Make certain that all covered functions are brought into compliance.
- Review new programs and functions to be sure that HIPAA is applied when needed.
- Assure that changes to the regulations are consistently applied.

Provide Consistency

By approaching compliance to HIPAA from the county level, rather than from individual departments, the County would be able to maintain an integrated, consistent approach to compliance.

- Policies and procedures will be consistent and complimentary.
- Usage and disclosure rules will be followed in a consistent way.
- Interaction with the public (Notice of Privacy, Accounting of disclosures, Complaints, Access to records, Accounting of disclosures, etc.) can be made to be united and consistent.
- All covered functions will be compliant, and changes to the regulations can be consistently applied to maintain compliance.

Limit Compliance Burden

As a Hybrid Entity, the County would be able to limit the burden associated with compliance.

- Most of the requirements of the Privacy Rule only apply to the health care component(s) of the hybrid entity and not to the parts of the entity that do not engage in covered functions.
- The exchange of Protected Health Information (PHI) between the Health Care Components of a Hybrid Entity is not considered a disclosure, so does not require accounting, authorizations, or Business Associate Agreements.
- While some policies and awareness training will still be required throughout the county as a whole, most efforts can be focused on the covered portions of the county.

Reduce Costs

By approaching compliance to HIPAA from the county level, as a Hybrid Entity, the County would reduce costs in several ways, such as:

HIPAA HYBRID ENTITY HEALTH CARE COMPONENTS

EL DORADO PHASE II: DETAILED HIPAA ANALYSIS

Requirement: *Designate Health Care Components*

As a Hybrid Entity, the County would be required to define and designate those parts of the County that engage in the covered functions and "business associate" functions and that are, therefore, part of the health care component((s). The County would also be required to document the designation as required by Sec. 164.530(j).

With respect to the components that perform covered functions, the County must include in its health care component(s) any component that would meet the definition of "covered entity" if it were a separate legal entity.

With respect to the components that perform "business associate" functions, the County may include or exclude them from its health care components. The components of a hybrid that may provide services to the component that performs covered functions, such as a portion of the legal or accounting departments of the entity, may be included in the health care component so protected health information can be shared with such components of the entity without requiring business associate agreements or individual authorizations. If such a component is excluded, a disclosure of protected health information from the health care component is the same as a disclosure outside the covered entity.

Documentation:

Formal Documentation of the Health Care Components will consist of:

- The "Phase I Assessment Interview Form" previously completed for each department.
- Amendments to the "Phase I Assessment Interview Form" reflecting further research
- The document "HIPAA Hybrid Entity Recommendation"
- The attached diagram named "El Dorado County Health Care Components"
- This Document
- Appropriate documentation of the structure and assignment of a privacy official.

Health Care Components:

Department covered in their entirety:

- **Public Health**
- **Mental Health**

  These departments are almost entirely covered functions. It would be inefficient to try to separate their non-covered functions. Both of these departments are designated Health Care Components, in their entirety.

Departments with some covered functions:

- **Risk Management**

  Risk Management has only one covered function, the Self-funded Health Plan (and its associated Health Plan Appeals Board). All other functions are either not Healthcare related, or not covered by the definition of PHI (such as employer functions). The Health Plan is already logically held separate from the other tasks performed, for confidentiality reasons. Policy should formalize this separation. The Health Plan and the Health Plan Appeals Board are Health Care Components, the remainder of Risk Management is not.
- **Community Services**

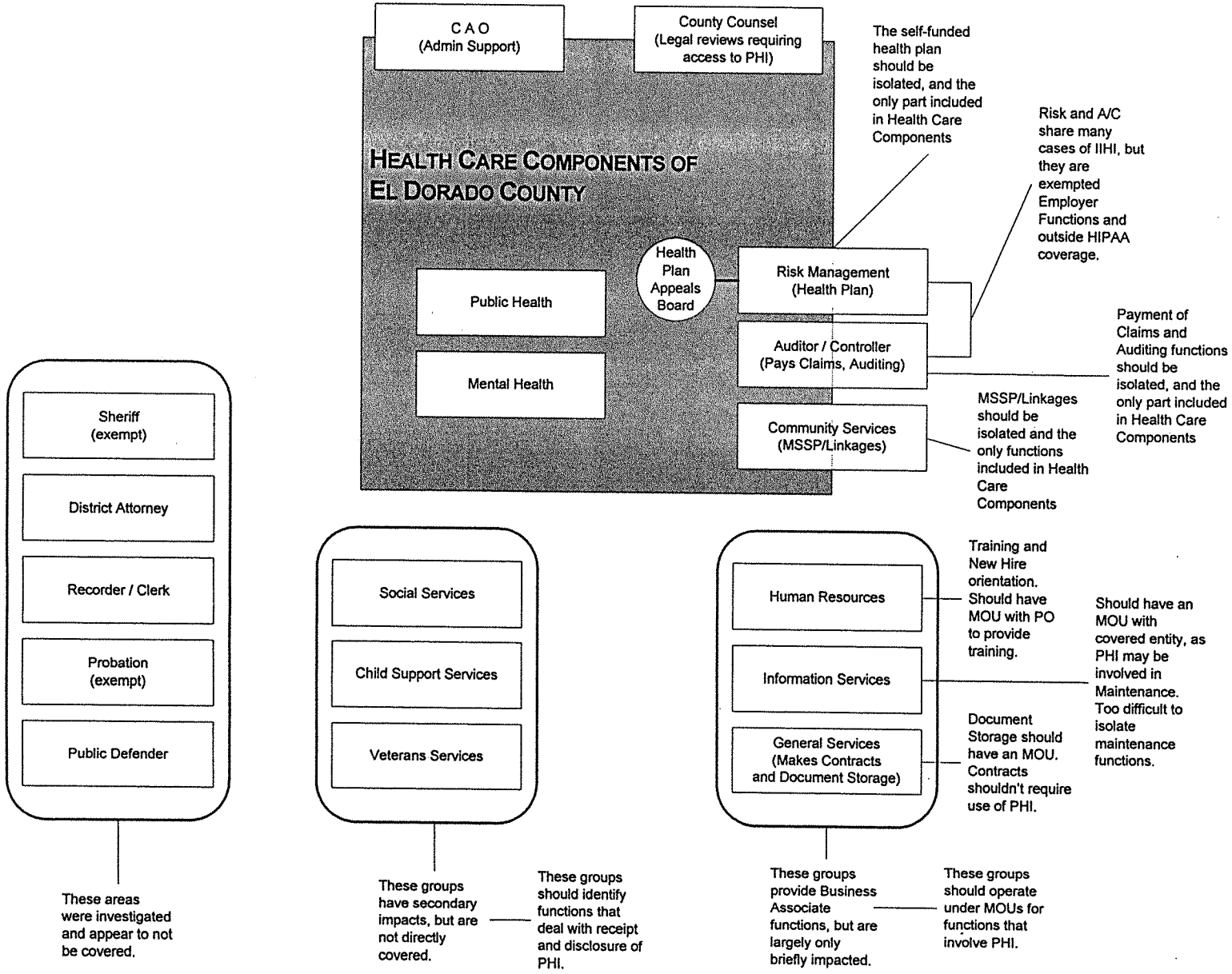
  Community Services has one covered function (MSSP). In addition, they have a program called Linkages that, although not a covered function, is closely related to MSSP. These functions should be separated by policy and included as Health Care Components. The remainder of Community Services would not be included.
- **Auditor/Controller**

  The Auditor/Controller's office has two affected functions. First, they handle health care payments (paying claims and receiving payments). They also audit other departments. While this would not be a covered function, it may cause a need for the auditor to have to access PHI. By including these functions, this exchange is no longer a disclosure requiring Business Associate agreements. These functions should be controlled by policy to prevent the sharing of PHI with other Auditor/Controller duties (except as allowed by HIPAA). To facilitate the

HIPAA HYBRID ENTITY HEALTH CARE COMPONENTS

EL DORADO PHASE II: DETAILED HIPAA ANALYSIS

Designation of Health Care Components of El Dorado County



17-0866 I 7 of 15

It is expected that this position would require full time attention in the initial implementation period. During this time, the Privacy Official will need to perform many "set-up" activities such as:

- Obtain the needed Privacy and HIPAA training,
- Work with the appropriate departments to create, get approval of, and implement policies and procedures,
- Work with the appropriate departments to create and get approval of the required Notification(s),
- Work with the appropriate departments to create and get approval of the required Authorization(s), Consents, Requests, and other required forms,
- Create standard approaches and Language to Business Associate Agreements,
- Work with the affected areas to properly amend existing contracts with Business Associates (and create written agreements where required with un-contracted groups or companies).
- Determine the application of State Preemptory law,
- Work with Human Resources and the appropriate departments to create and implement County-wide training (and Agency specific training where needed)

Designate a Compliance Advisory Committee to advise the Privacy Official

The Privacy Official must take into account many things in addition to the HIPAA regulation, including, but not limited to:

- Employment Law and Practices,
- The realistic working environment and requirements of each agency,
- Other laws and regulations that apply to individual programs and agencies,
- Relationships with other entities and companies.

Although not a requirement, an advisory group is allowed. Due to the impact of this regulation, an advisory board for the Privacy Official would provide a mechanism for the areas that must comply to have a say in how this is accomplished, avoid the unnecessary feelings that the "burden" compliance is simply being thrust upon each agency and the associated resistance to change that creates, and provide a mechanism to foster the cultural change required for compliance to become something we are (rather than something we do).

The actual implementation should be designated by policy. However, this committee should be chaired by the Privacy Official and should be composed of Department Heads (or their designates) from each department with a designated Health Care Component, from Information Systems (to provide technical advise), from the CAO, from County Counsel and from Human Resources.

DEPARTMENT OF PUBLIC HEALTH SUMMARY

EL DORADO PHASE II: DETAILED HIPAA ANALYSIS

Individual areas reviewed:

Policies and Procedures:

Findings:

The Department of Public Health reviewed their existing written policy, compared to the HIPAA Privacy Final Rule. In all applicable cases, no written policy exists, within Public Health, that would satisfy the regulations. Some policies (such as Whistleblower and Sanctions Policies) are covered by County-wide policies maintained in other departments.

Recommendations:

Once County policies are in place, the Department must:

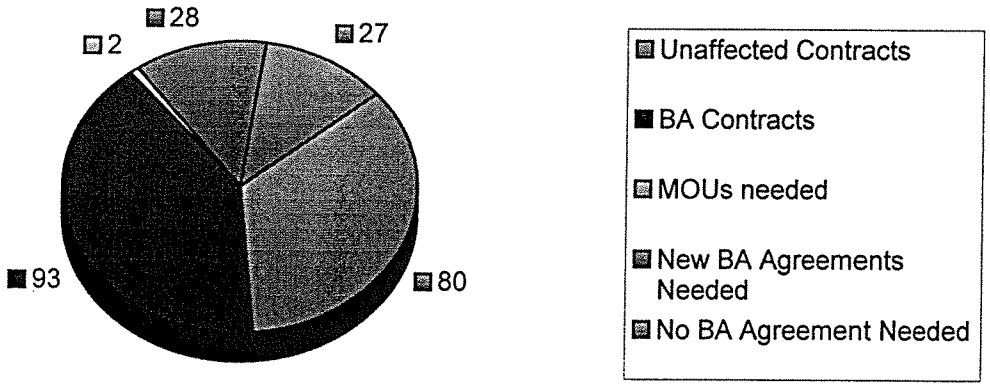
- Draft Department Policies to support and apply County HIPAA Policy,
- Individual divisions should review their procedures, be sure they are documented, and be sure they comply with and reference appropriate HIPAA Policy,

Contracts, MOUs and other Business Relationships:

Findings:

The Department of Public Health inventoried all contracts and informal (un-contracted) business relationships. This inventory was then reviewed to determine which relationships were Business Associates and required future action. The Department maintains 173 written contracts. Of these, 93 are Business Associates of some form (leaving 80 unaffected). In addition to these contracts, the Department has identified 55 business relationships that involve Health Information, but do not have a contract in place. Of these, the department has identified 28 as potential Business Associates that will now require a Business Associate Agreement (leaving 27 which do not require any action). Finally, the Hybrid Entity structure proposed would create a need for at least 2 MOUs to contain Business Associate assurances (IS and the new Privacy Official).

Public Health



Recommendations:

Once County standard Business Associate Agreement language is created, the Department must:

- Prioritize the Business Relationships based on importance and contract terms,
- Review each of the identified contracts to determine the needed language, and amend the affected contracts,
- Review each affected informal relationship to determine what language a Business Associate agreement should contain, and execute a Business Associate Agreement.

DEPARTMENT OF MENTAL HEALTH SUMMARY

EL DORADO PHASE II: DETAILED HIPAA ANALYSIS

Summary:

Findings:

The Department of Mental Health is almost entirely covered functions. It would be inefficient to try to separate their non-covered functions. The Department of Mental Health is designated a Health Care Component, in its entirety.

The detailed analysis of the Department of Mental Health is nearly complete. The Department has completely inventoried all contracts and software applications. Policies have been reviewed against the regulation to determine policy and procedure requirements. The Contracts and Business Relationships are being reviewed to identify Business Associate Relationships. The Software is being reviewed for impacts and risks.

Recommendations:

The Department will need to complete the detailed analysis. The remaining tasks include conducting the Physical Security walk-throughs, completing the contract reviews and completing the Software Review.

In Phase III, the department will need to:

- Review and Amend 29 contracts,
- Create and execute 2 new MOUs,
- Create and document policies to support and implement County HIPAA Policy,
- Document existing procedures and ensure that they reference and follow appropriate policy,
- Install physical and electronic safeguards determined by the walk-throughs and software review

Software and Databases:

Findings:

The Department of Mental Health inventoried all of the databases and software systems they use to create and maintain health information. This list is being reviewed to determine which systems transmit Protected Health Information using any of the HIPAA identified transactions. In addition, the list is being reviewed to determine which applications and databases require physical or electronic safeguards because of their location or accessibility.

Recommendations:

The Department should:

- Complete the software review that is underway,
- Identify and implement physical and procedural safeguards to secure PHI stored on department PCs,
- Work with IS to determine and implement electronic safeguards as needed,
- Work with IS and the Privacy Official to ensure that transmitted PHI is compliant with HIPAA TCI rules. In cases where PHI is only remotely accessed, and the software and data reside on other systems, documentation should be obtained concerning the compliance efforts of the entity in control of the software and data.

Physical Safeguards:

Findings:

The Department of Mental Health has not yet begun physical walk-throughs of locations used by the Department. These walk-throughs will be used to determine where records are stored, computers can be accessed, and information can be transmitted (faxes and printers). They will also identify where physical safeguards such as Fire extinguishers, locking file cabinets and limited-access work areas are already in place. Finally, they will be used to determine if procedures used affect physical security of the data (passwords written on monitors, clean desk requirements, visitors excluded or escorted, etc.). This data will be used to determine where additional safeguards may be required to ensure the confidentiality of PHI used at each facility.

Recommendations:

The Department should:

- Conduct the Physical Walk-throughs,
- Identify areas where PHI is at risk, and prioritize these by risk,
- Identify areas that may be made more secure by Policy or Procedure change, and implement those changes,
- Determine where addition physical security is required and determine final costs.

DEPARTMENT OF COMMUNITY SERVICE SUMMARY

EL DORADO PHASE II: DETAILED HIPAA ANALYSIS

Individual areas reviewed:

Policies and Procedures:

Findings:

The Department of Community Services is currently reviewing their existing written policy, compared to the HIPAA Privacy Final Rule. While written policies exist within the department, few are expected to have completely compliant language that would satisfy the regulations. Some policies (such as Whistleblower and Sanctions Policies) are covered by County-wide policies maintained in other departments.

Recommendations:

Once County policies are in place, the Department must:

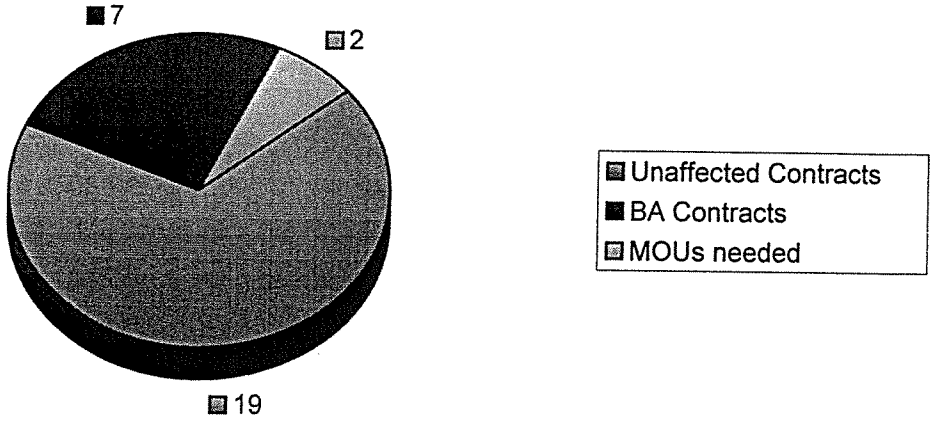
- Draft or revise Department Policies to support and apply County HIPAA Policy,
- Draft an internal policy denoting the covered status of the AP and selected Auditing Functions, and how a separation between functions will be maintained.
- Review the procedures that cover AP and Auditing, be sure they are documented, and be sure they comply with and reference appropriate HIPAA Policy,

Contracts, MOUs and other Business Relationships:

Findings:

The Department of Community Services inventoried all contracts and informal (un-contracted) business relationships that may have a connection or impact in the covered areas. This inventory was then reviewed to determine which relationships were Business Associates and required future action. The Department reviewed 26 written contracts. Of these, 7 have been found to be a Business Associates (leaving 19 unaffected). In Addition, the Hybrid Entity structure proposed would create a need for at least 2 MOUs to contain Business Associate assurances (IS and the new Privacy Official).

Community Services



Recommendations:

Once County standard Business Associate Agreement language is created, the Department must:

- Prioritize the Business Relationships based on importance and contract terms,
- Review each of the identified contracts to determine the needed language, and amend the affected contracts,

DEPARTMENT OF RISK MANAGEMENT SUMMARY

EL DORADO PHASE II: DETAILED HIPAA ANALYSIS

Summary:

Findings:

The Department of Risk Management has only one covered function, the Self-funded Health Plan (and its associated Health Plan Appeals Board). All other functions are either not Healthcare related, or not covered by the definition of PHI (such as employer functions). The Health Plan is already logically held separate from the other tasks performed, for confidentiality reasons. Policy should formalize this separation. The Health Plan and the Health Plan Appeals Board are Health Care Components, the remainder of Risk Management is not.

The detailed analysis of the Risk Management is nearly complete. The Department has completely inventoried all contracts, business relationships, and software applications that relate to the Health Plan. Policies have been reviewed against the regulation to determine policy and procedure requirements. A Physical Safeguard walk-through has been conducted. The Contracts and Business Relationships have been reviewed to identify Business Associate Relationships. The Software is being reviewed for impacts and risks.

In addition to the standard inventories, Risk Management operates the Health Plan under a controlling Health Plan Document. Some language in this document appears to be inconsistent with HIPAA, and some HIPAA requirements may need additions to this document. A legal review of this document should be performed to determine HIPAA impacts, determine Preemptive California Law that may override HIPAA requirements, and recommend alterations that will be needed. Caution should be exercised in any changes to this document, to be sure that proper procedure is followed. Changes to this document will have implications outside of HIPAA, including employee relations and County liability.

Recommendations:

The Department will need to complete the Software Review and verify other detail results.

In Phase III, the department will need to:

- Obtain a legal review of the Health Plan Document to determine HIPAA impacts and recommend changes. The method for altering this document should be reviewed, and appropriate steps taking to complete that procedure.
- Review and Amend 10 contracts,
- Create and execute 2 new MOUs,
- Create and document policies to support and implement County HIPAA Policy,
- Draft an internal policy denoting the covered status of the Health Plan, and how a separation between functions will be maintained.
- Document existing procedures and ensure that they reference and follow appropriate policy,
- Install physical and electronic safeguards determined by the walk-throughs and software review

Recommendations:

Once County standard Business Associate Agreement language is created, the Department must:

- Prioritize the Business Relationships based on importance and contract terms,
- Review each of the identified contracts to determine the needed language, and amend the affected contracts,
- Once the Privacy Official is designated, the Department should create an appropriate MOU to define the relationship and clarify roles and responsibilities.
- Once Department Policies and Procedures have been established, the Department should review and amend their MOU with IS to properly safeguard PHI that IS may have access to because of their support position.

Software and Databases:

Findings:

The Department of Risk Management inventoried all of the databases and software systems they use to create and maintain health information. This list is being reviewed to determine which systems transmit Protected Health Information using any of the HIPAA identified transactions. In addition, the list is being reviewed to determine which applications and databases require physical or electronic safeguards because of their location or accessibility.

Recommendations:

The Department should:

- Complete the software review that is underway,
- Identify and implement physical and procedural safeguards to secure PHI stored on department PCs,
- Work with IS to determine and implement electronic safeguards as needed,
- Work with IS and the Privacy Official to ensure that transmitted PHI is compliant with HIPAA TCI rules. In cases where PHI is only remotely accessed, and the software and data reside on other systems, documentation should be obtained concerning the compliance efforts of the entity in control of the software and data.

Physical Safeguards:

Findings:

The Department of Risk Management has conducted a physical walk-through of the location used by the Department for Health Plan Activities.

Recommendations:

The Department should:

- Identify areas where PHI is at risk, and prioritize these by risk,
- Identify areas that may be made more secure by Policy or Procedure change, and implement those changes,
- Determine where addition physical security is required and determine final costs.

AUDITOR / CONTROLLER DEPARTMENT SUMMARY

EL DORADO PHASE II: DETAILED HIPAA ANALYSIS

Individual areas reviewed:

Policies and Procedures:

Findings:

The Auditor / Controller Department is currently reviewing their existing written policy, compared to the HIPAA Privacy Final Rule. While written policies exist within the department, few are expected to have completely compliant language that would satisfy the regulations. Some policies (such as Whistleblower and Sanctions Policies) are covered by County-wide policies maintained in other departments.

Recommendations:

Once County policies are in place, the Department must:

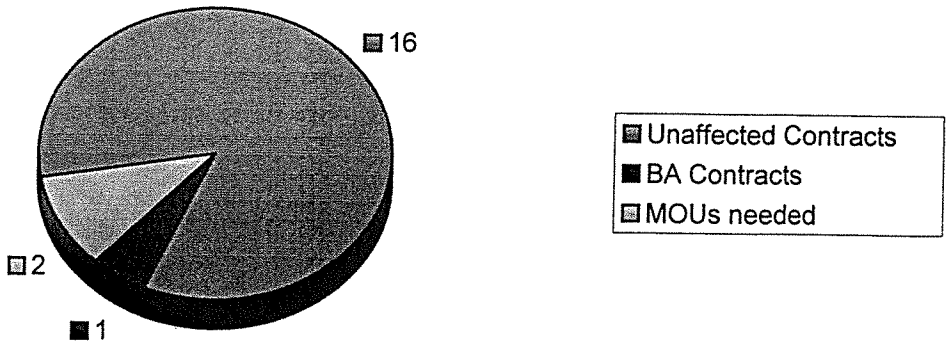
- Draft or revise Department Policies to support and apply County HIPAA Policy,
- Draft an internal policy denoting the covered status of the AP and selected Auditing Functions, and how a separation between functions will be maintained.
- Review the procedures that cover AP and Auditing, be sure they are documented, and be sure they comply with and reference appropriate HIPAA Policy,

Contracts, MOUs and other Business Relationships:

Findings:

The Auditor / Controller Department inventoried all contracts and informal (un-contracted) business relationships that may have a connection or impact in the covered areas. This inventory was then reviewed to determine which relationships were Business Associates and required future action. The Department reviewed 17 written contracts. Of these, only 1 was found to be a Business Associate (leaving 16 unaffected). In Addition, the Hybrid Entity structure proposed would create a need for at least 2 MOUs to contain Business Associate assurances (IS and the new Privacy Official).

Auditor / Controller



Recommendations:

Once County standard Business Associate Agreement language is created, the Department must:

- Review the contract to determine the needed language and amend the contract,
- Once the Privacy Official is designated, the Department should create an appropriate MOU to define the relationship and clarify roles and responsibilities.