PURPOSE

Shasta County is committed to ensuring the confidentiality, integrity, and availability of all Electronic Protected Health Information (EPHI) that designated covered components of the County create, receive, maintain, or transmit in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191) and the standards of the Security Rule promulgated by the federal Department of Health and Human Services (45 CFR Part 164). This administrative policy is adopted in order to implement policies and procedures required by the Security Rule (45 CFR 164.316). This administrative policy applies to protected EPHI created, received, maintained, or transmitted by the designated covered components of the County on or after April 20, 2005. This policy is also established to protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, to protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required, and to ensure compliance of the workforce of the County's designated covered components with the Security Rule.

DEFINITIONS

All definitions in the Security Rule as set forth in 45 CFR 164.304 shall apply to this administrative policy unless otherwise indicated.

SCOPE

Shasta County is a hybrid entity, as defined in 45 CFR 164.504. This administrative policy applies only to the County's designated covered components, which are:

- The Department of Public Health, excluding the Women, Infants, and Children (WIC) program;
- The Department of Mental Health, including the Alcohol and Drug Programs;
- The Offices of the Director and of the Business and Support Services Branch of the Health and Human Services Agency;
- The Office of County Counsel; and
- The Information Technology Department.

The designated covered components may not share EPHI with the non-covered components of the County, nor each other, unless specifically permitted by the Security Rule. It is the responsibility of the department or agency head of each designated covered component to assure that his/her workforce complies with this administrative policy. The department head of a designated covered component may adopt additional departmental policies and procedures to comply with the Security Rule and more

stringent state laws regarding protecting and ensuring the confidentiality, integrity, and availability of all EPHI created, received, maintained, or transmitted by the designated covered component.

BACKGROUND

County departments designated as covered components must comply with the Security Rule. They must also comply with California laws and regulations pertaining to the use and disclosure of EPHI and individually identifiable health information, unless such state laws and regulations are preempted by the HIPAA Security or Privacy Rules.

POLICY

1. County Security Officer

The County HIPAA Security Officer (Security Officer) is the County Executive Officer or his/her designee. The Security Officer shall be deemed the "security official" for the purposes of 45 C.F.R. §164.308(a)(2).

2. Authorization to Use or Disclose EPHI

The County's designated covered components shall obtain an individual's authorization to use or disclose EPHI when required by HIPAA, the Privacy Rule, or the Security Rule.

3. Flexibility of Approach

When creating, receiving, maintaining, or transmitting EPHI covered by the Security Rule, the County's designated covered components shall ensure the confidentiality, integrity, and availability of all EPHI; protect against any reasonably anticipated threats or hazards to the security or integrity of all EPHI; protect against reasonably anticipated uses or disclosures of all EPHI which are not permitted or required; and ensure compliance with the Security Rule by the designated covered components' employees.

Each covered component which uses or discloses EPHI has a unique organizational structure and performs various functions that require different levels of access to EPHI. Further, the responsibilities assigned to those functions vary and cannot be determined based on job title or description. It is the responsibility of each covered component that uses and discloses EPHI to

determine the level of access required to perform particular functions and responsibilities within that department or agency and document that determination.

The covered components may use any security measures that allow the covered components to reasonably and appropriately implement the security standards and implementation specifications as specified in HIPAA and the Security Rule. In deciding which security measures to use, each covered component must take into account: (i) the size, complexity, and capabilities of the covered component; (ii) the covered component's technical infrastructure, hardware, and software security capabilities; (iii) the costs of security measures; and (iv) the probability and criticality of potential risks to EPHI.

4. Risk Analysis and Management

Risk Analysis. The County's designated covered components shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by that component.

The Department of Public Health, Department of Mental Health, the Office of County Counsel, and the Information Technology Department shall complete, prior to April 20, 2005, the Business Impact Assessment, which is a supplemental survey to be used in conjunction with the Business Continuity Plan Generator software package provided by the County's Information Technology Department. The Offices of the Director and of the Business and Support Services Branch of the Health and Human Services Agency shall complete the Business Impact Assessment prior to December 31, 2008. The Business Impact Assessment will provide an assessment of the impact that may occur from the loss of confidentiality, integrity, or availability of EPHI and can assist in determining the cost effectiveness of protection measures.

Risk Management. The covered components shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule.

a) The covered components shall implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

b) The covered components shall assess the relative criticality of specific applications and data in support of other contingency plan components.

c) In response to environmental or operational changes affecting the security of EPHI, the covered components shall perform a periodic technical and non-technical evaluation that establishes the extent to which the covered components meet these security policies and procedures as required by the Security Rule.

5. Authorization, Supervision, and Workforce Clearance

a) The covered components shall implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.

b) The covered components shall implement procedures to determine that the access of a workforce member to EPHI is appropriate.

c) The covered components shall implement policies and procedures for granting access to EPHI through access to a workstation, transaction, program, process, or other mechanism. The covered components shall implement policies and procedures that (based upon the component's access authorization policies) establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process, including procedures to terminate access to EPHI.

6. Security Incident Procedures

The County's designated covered components shall implement policies and procedures to address breach of security incidents. The covered components shall identify and respond to suspected or known breach of security incidents; mitigate, to the extent practicable, harmful effects of breach of security incidents that are known to the covered components; and document breach of security incidents and their outcomes.

7. Contingency Plan/Business Resumption Plan

The County's designated covered components shall establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (such as fire, vandalism, system failure, and natural disaster) that damages systems containing EPHI. The Department of Public Health, Department of Mental Health, and the Information Technology Department shall complete, prior to December 31, 2005, the Business Continuity Plan Generator software package provided by the County's Information Technology Department. The Offices of the Director and of the Business and Support Services Branch of the Health and Human Services Agency shall

complete the Business Continuity Plan Generator software package prior to December 31, 2008. The Business Continuity Plan Generator will, at a minimum, address the following activities:

a) Data backup plan. The covered components shall establish and implement procedures to create and maintain retrievable exact copies of EPHI.

b) Disaster recovery plan. The covered components shall establish (and implement as needed) procedures to restore any loss of data.

c) Emergency mode operation plan. The covered components shall establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.

d) Testing and revision procedures. The County's designated covered components shall implement procedures for periodic testing and revision of contingency plans.

e) Applications and data criticality analysis. Assess the relative criticality of specific applications and data in support of other contingency plan components.

8. Evaluation

The County's designated covered components shall, in accordance with the Security Rule, perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI.

9. Physical Safeguards

The County's designated covered components shall, in accordance with the Security Rule implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed, as follows:

a) Establish 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) Implement policies and procedures to safeguard facilities and the equipment therein from unauthorized physical access, tampering, and theft.

c) 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) Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security.

e) Implement policies and procedures 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 EPHI.

f) Implement physical safeguards for all workstations that access EPHI to restrict access to authorized users.

g) Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.

h) Implement policies and procedures to address the final disposition of EPHI and/or the hardware or electronic media on which it is stored.

i) Implement procedures for removal of EPHI from electronic media before the media are made available for re-use.

j) Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

k) Create a retrievable, exact copy of EPHI, when needed, before movement of equipment.

10. Technical Safeguards

The County's designated covered components shall, in accordance with the Security Rule implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights, as follows:

a) Assign a unique name and/or number for identifying and tracking user identity.

b) Establish (and implement as needed) procedures for obtaining EPHI during an emergency.

c) Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.

d) Implement policies and procedures to protect EPHI from improper alteration or destruction.

e) Implement procedures to verify the identity of a person or entity seeking access to EPHI, such as passwords and unique user IDs.

f) Implement technical security measures to guard against unauthorized access to EPHI transmitted over an electronic communications network.

11. Preemption Analysis

There are situations when California law may be more "stringent" with regard to the security of EPHI than HIPAA or the Security Rule. When a designated covered component requires a preemption analysis to determine whether HIPAA and the Security Rule, or state law is more stringent, the matter shall be brought to the Security Officer and County Counsel for a determination.

12. Business Associates

All persons or entities that contract as a Business Associate of a designated covered component of the County shall be bound by HIPAA language contained in any new contract or amended contract signed on or after April 20, 2005, as required by the Security Rule. The addendum is attachment D to Administrative Policy 6-101, *Shasta County Contracts Manual*.

13. Sanctions

A violation of this Administrative Policy and/or the Security Rule shall be grounds for discipline, as provided for in the Shasta County Personnel Manual and any applicable Memorandum of Understanding.

14. Training

Each designated covered component must document the following training actions:

a) On or before April 20, 2005, the Department of Public Health, Department of Mental Health, the Office of County Counsel, and the Information Technology Department shall have a documented plan (submitted to the Security Officer) to provide security awareness to each member of their workforce by June 30, 2005, including periodic security updates/reminders, related to HIPAA, the Security Rule, and this Administrative Policy, as necessary and appropriate to carry out the functions within the respective departments. On or before December 31, 2008, the Offices of the Director and of the Business and Support Services Branch of the Health and Human Services Agency shall have a documented plan (submitted to the Security Officer) to provide security awareness to each member of the Agency's workforce by December 31, 2008, including periodic security updates/reminders, related to HIPAA, the Security Rule, and this Administrative Policy, as necessary and appropriate to carry out the functions within the Agency.

b) Each new workforce member shall receive the training, as described above, within a reasonable time and in no event more than 90 days after joining the workforce of a designated covered component.

c) Each workforce member whose functions are impacted by a material change in HIPAA, the Security Rule, this Administrative Policy, or by a change in position or job description, must receive the training, as described above, within a reasonable time and in no event more than 90 days after the change becomes effective.

15. Documentation

a) The County shall maintain policies and procedures implemented to comply with the HIPAA Security Rule in written (which may be electronic) form; and if an action, activity, or assessment is required by the Security Rule to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

b) The County shall retain the policies and procedures and other required documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.

c) The County shall make the policies and procedures and other required documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

d) The County shall periodically review the policies and procedures implemented to comply with the HIPAA Security Rule, and update them as needed, in response to changes in HIPAA, changes in the Security Rule, changes in any other laws or regulations, and environmental or operational changes affecting the security of EPHI.

16. E-mail Containing EPHI

Each designated covered component that allows employees to use e-mail to transmit EPHI shall include in the body of the e-mail a confidentiality notice containing the following language:

> *This e-mail, and any attachments, contains information that is, or may be covered by, the Electronic Communication Privacy Act, Title 18 U.S.C 2510-2521, and is also confidential and proprietary in nature. If you received this e-mail in error, please be advised that you are legally prohibited from retaining, using, copying, distributing, or otherwise disclosing this information in any manner. If you have received this e-mail in error, please contact sender indicating that you received this communication in error, and then immediately delete it. Thank you in advance for your cooperation.*

RESPONSIBLE DEPARTMENTS/PERSONS

County Administrative Office
Office of County Counsel
Shasta County HIPAA Privacy Officer
Shasta County HIPAA Security Officer

REFERENCES

BOS Policy Resolution No. 2012-07--11/13/12 (Amended)
Administrative Update--07/13/2012
BOS Policy Resolution No. 2009-03--5/12/09 (Amended)
BOS Policy Resolution No. 2008-02--3/4/08 (Amended)
BOS Policy Resolution No. 2007-2--4/24/07 (Amended)
BOS Policy Resolution No. 2005-2--4/19/05