BOARD POLICY 2210

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

ADMINISTRATION

HIPAA/CMIA PRIVACY POLICY

A. Purpose

Medical information regarding an individual is protected by the Confidentiality of Medical Information Act (CMIA), Calif. Civil Code, Section 56 et. seq., and may be protected by the Health Insurance Portability Accountability Act (HIPAA), Public Law 104-196. It is the intent of the South Orange County Community College District ("District") to protect the privacy of medical information in accordance with these laws.

This policy is intended to do the following:

1. Serve as a foundation for the District's privacy practices;

2. Describe what health or health-related information is considered private;

3. Outline, in part, individual rights regarding private medical information (PMI), see Section B.8 for definition of PMI;

4. Designate the HIPAA Privacy Officer and Complaint Official; and

5. Require employee training in Protected Health Information (PHI). PHI is defined as "individually identifiable information, in electronic, paper or oral form, which is created or received by or on behalf of the District or its health care components."

The colleges and the District Office shall also be responsible for developing additional policies and procedures as necessary to safeguard PMI. Such policies are subject to approval by the Privacy Officer and must be consistent with this policy. Any and all policies and procedures relating to the subject matter of the policy in existence at the time this policy is adopted by the District's Board of Trustees shall be subject to this policy. As part of the implementation of this policy, the Privacy Officer shall review and revise any and all existing District policies and procedures relating to the subject matter of this policy, including but not limited to those policies and procedures utilized by Saddleback College's Student Health Center and Irvine Valley College's Health and Wellness Center. This Policy pertains to all District individuals who have access to, use, or disclose PMI. The District's Privacy Officer develops and implements policies and procedures with respect to HIPAA compliance and receives HIPAA non-compliance allegations.

B. Definitions

1. Authorization

Authorization means the execution of a written document required for the District to use or disclose PMI. Authorization must be obtained in advance of use or disclosure except for purposes of emergency treatment. The Authorization attached hereto as Exhibit "A" to this Policy is the only form approved for use by District employees.

2. Business Associate

A Business Associate (BA) is a person or an entity not a member of the District's workforce who performs a function and/or activity for a Covered Entity involving the use, disclosure or creation of PHI. The function and/or activity performed does not have to be a covered function and/or activity, but must be a function and/or activity that the Covered Entity would have had to perform themselves. All entities that perform as a BA of the District will be required to enter into a BA Agreement with the District. A BA could be, for example, a copy service that has access to PHI, or a flexible spending account's third party administrator.

3. Covered Entity

A "Covered Entity" is a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form in connection with a HIPAA transaction as defined by HIPAA (45 C.F.R. § 160.103).

4. Covered Functions

Covered functions refers to those functions of a covered entity, the performance of which subjects the covered entity to the HIPAA requirements, i.e. use, disclosure, or creation of PHI.

5. Hybrid Entity

A hybrid entity is a single legal entity, portions of which are covered entities within the meaning of the HIPAA that perform covered functions. The District is such a hybrid entity (45 C.F.R. § 160.103). The District's operations which perform covered functions and, therefore, are designated as health care components, are: the District's Student Health Center at Saddleback College and the Health and Wellness Center at Irvine Valley College, which engage in standard electronic HIPAA transactions.

6. Limited Data Sets

PHI that excludes the direct identifiers of the individuals, relatives, employers, or household members of the individual, listed below in subsections (a) through (p), constitutes a limited data set. Limited data sets may be used or disclosed, without written authorization, where three criteria are met: (1) the use and/or disclosure is only for purposes of research, public health, or health care operations; (2) the covered entity obtains a data use agreement from the recipient whereby the recipient agrees to limit the use of the limited data set to the purpose allowed by the rules, to limit who can use or receive the data and not to re-identify the data or contact the individuals; and (3) where the covered entity does not have knowledge that the remaining information can be used to identify an individual.

a. Names;

b. Postal address information, other than town or city, State, and zip code;

c. Telephone numbers;

d. Fax numbers;

e. Electronic mail addresses;

f. Social security numbers;

g. Medical record numbers;

h. Health plan beneficiary numbers;

i. Account numbers;

j. Certificate/license numbers;

k. Vehicle identifiers and serial numbers, including license plate numbers;

l. Device identifiers and serial numbers;

m. Web Universal Resource Locators (URLs);

n. Internet Protocol (IP) address numbers;

o. Biometric identifiers, including finger and voice prints; and

p. Full face photographic images and any comparable images.

7. Notice of Privacy Practices

The District shall issue a "District Notice of Privacy Practices" for its Covered Entities. The notice shall specify individual rights under HIPAA as well as the District's contact information and the method of filing a complaint.

8. Private Medical Information

For purposes of this policy, Private Medical Information (PMI) includes medical information covered by both HIPAA and the CMIA. PMI is any information that could specifically identify an individual's past, present, or future health condition. For example, medical billing records and a doctor's note. As a precautionary measure, all medical information shall be treated by District employees as PMI unless it can be clearly demonstrated to the Privacy Officer that said information is outside the scope of HIPAA or the CMIA.

9. Security

Security in this policy is defined as all measures taken by the District and its agents, contractors, officers and employees to insure that PMI is protected in a manner which complies with the HIPAA and the CMIA. Security measures include, but are not limited to, policies, procedures, practices, directives, manuals, training, and methods as they relate to compliance with HIPAA and the CMIA. Security measures may also include mechanical and technological protections such as locks, secure access rooms and containers, computer hardware and software with security levels and protocols, secure communication devices and settings, and any other method, device or practice that limits improper access to PHI.

C. Policy

1. Allowable Uses/Disclosures of PHI

PMI shall only be used and/or disclosed on a need-to-know basis or where authorization has been received. In general, PMI may not be used or disclosed by the District without an authorization except in the following circumstances:

a. When the information is provided to the individual whose PMI it is;

b. When the information is required by the United States Secretary of Health and Human Services to investigate compliance with the HIPAA;

c. When the information is requested pursuant to a valid subpoena;

d. When the information is part of a limited data set as defined above;

e. When the information is provided to a business associate (safeguarded by a business associate agreement);

f. When the information is provided to another government agency that is administering a public benefit health plan;

g. When the individual, whose PMI is being disclosed, has been given an opportunity to contest the disclosure of PMI in advance;

h. When the information is used for public health activities authorized by law;

i. When disclosure of the information is necessary to report child abuse or neglect as authorized by law;

j. When the information is provided to a person who may have been exposed to a communicable disease;

k. When the information is disclosed to a government authority, which is authorized by law to receive reports of abuse, neglect, or domestic violence, because there is reasonable belief that the individual is a victim of abuse, neglect, and/or domestic violence;

l. When the information is used for law enforcement purposes;

m. When the District believes that disclosure of the information is necessary to avert a serious threat to health or safety;

n. When the information is used for government programs providing public benefits;

o. When the information is required for worker's compensation purposes;

p. When the information is used or disclosed to a business associate or to an institutionally related foundation for the purpose of raising funds for its own benefit. PHI released can only be in the form of demographic information relating to an individual and dates of health care provided to an individual used for fundraising;

q. When the information is disclosed for underwriting and related purposes.

2. Internal Audit

In order to ensure appropriate use and disclosure PMI, each college and he District Office shall audit itself on a semi-annual basis. Each college and the District Office shall identify PMI in its possession, then determine whether there are potential HIPAA and CMIA violations and develop a plan for correction. Upon completion of the audit, the information shall be delivered to the District Privacy Officer. The Privacy Officer shall work with each college and the District Office creates a Remediation Plan, if necessary.

3. Individual Rights

An individual has the following rights as to his or her PHI protected under HIPAA. Individuals covered by HIPAA have the following rights:

a. The right to request restrictions on certain uses and disclosures of protected health information as provided by 45 C.F.R. § 164.522(a);

b. The right to receive his or her PHI confidentially as provided by 45 C.F.R. § 164.522(b), as applicable;

c. The right to inspect and copy his or her PHI held in the covered entity's designated record set as provided by 45 C.F.R. § 164.524;

d. The right to request amendments to his or her PHI held in the covered entity's designated record set as provided by 45 C.F.R. § 164.526; and

e. The right to receive an accounting of disclosures of protected health information as provided by 45 C.F.R. § 164.528.

For individually identifiable medical information protected by the CMIA, but not HIPAA, an employee shall have the right to review and copy his or her medical information.

4. District Privacy Official and Contact Person

The District Privacy Official is the Vice Chancellor of Technology and Learning Services. The Privacy Official is responsible for resolving complaints under HIPAA and/or the CMIA. This official shall be identified as the person to receive complaints of alleged HIPAA and/or CMIA violations. Specific duties include, but are not limited to:

a. Pursuant to HIPAA, develop privacy policies and procedures and the Notice of Privacy Practice;

b. Develop training documents for the workforce on policies and procedures regarding PHI;

c. Set up a complaint process and sanctions;

d. Track all PHI;

e. Ensure policies are implemented for determining when an individual can inspect, copy, amend, or request restrictions on their PHI disclosures;

f. Receiving complaints from individuals concerning violations of HIPAA and/or CMIA and requirements;

g. Logging all complaints received and tracking the disposition of the complaints;

h. Reviewing complaints for allowable uses and disclosures and disposing of complaints that identify allowable uses and disclosures;

i. Reviewing complaints for non-HIPAA and/or non-CMIA related issues and referring the individuals to the appropriate organization, if any;

j. Identifying and investigating all HIPAA and/or CMIA-related complaints including allegations of: inappropriate use or disclosure of PMI; inappropriate disposal of PMI; denial of access to PMI; denial of amendments to PMI;

k. Coordinating and collaborating with members of the workforce to investigate and develop actions to resolve the complaints;

l. Resolving complaints, seeking approval of the resolution (from the complainants) and overseeing implementation of the resolution; Resolutions can include changes in business practices or information technology changes; personnel actions; contract changes or terminations, etc.;

m. Serving as the District's liaison with the federal and/or state government with respect to any inquiries into HIPAA and/or CMIA privacy violation complaints.

The District's Contact Person for complaints concerning HIPAA and/or the CMIA, as well as questions regarding the Notice of Privacy Practices is the Vice Chancellor of Technology and Learning Services.

5. Sanctions and Penalties

Employees may be subject to discipline, up to and including termination for violations of this policy, which includes the inappropriate use or disclosure of PMI, in accordance with existing provisions of law, policies of the Board of Trustees, or applicable collective bargaining agreements.

In addition, federal authorities may sanction employees and the District for violations of the HIPAA privacy rule as follows:

a. Civil penalties of not more than $100 per incident. Not more than $25,000 per person, per calendar year, per standard;

b. Criminal penalties for violations of the Privacy Rule:

1) A person who knowingly and in violations of the privacy rule either (a) obtains individually identifiable health information relating to an individual; or (b) discloses individually identifiable information to another person may have a criminal penalty assessed against them. Any violator may be fined up to $50,000 or imprisoned for up to one (1) year, or both;

2) Where a known violation is committed under false pretenses, the person may be fined up to $100,000 or imprisoned for up to five (5) years, or both;

3) Where a known violation is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a person can be fined up to $250,000, and/or incarcerated for not more than ten (10) years.

Any violation of CMIA that results in economic loss or personal injury to a patient is punishable as a misdemeanor. Any person and/or entity that negligently, knowingly, or willfully disclose medical information, in violation of CMIA, may be assessed fines or civil penalties.

6. Training

The District shall train employees so that they understand their obligations under this policy. The training requirement may be satisfied by providing new employees with a copy of this privacy policy and documenting that new members

have reviewed the policies. From time to time, the District may provide training through live instruction, video presentations, or interactive software programs.

7. Audit and Compliance

Each college and the District Office is responsible for compliance with this policy. The Privacy Officer may, in his or her discretion, audit and examine the procedures and practices of any college and the District Office to ascertain compliance with the requirements of this policy.