MONTEREY COUNTY DISTRICT ATTORNEY'S OFFICE POLICY MANUAL	**POLICY NO**. 1.42 **EFFECTIVE DATE: 05/16/03** **PAGE** 1 **OF** 3
SUBJECT: **HIPAA COMPLIANCE POLICY**	**BY: Dean D. Flippo** **District Attorney**

HIPAA is an acronym used for a federal act called the "Health Insurance Portability and Accountability Act of 1996."

HIPAA came into being due to concerns by citizens about threats to their individual privacy. Specifically, people were concerned that electronically stored medical records might be transmitted carelessly from one business or government agency to another or that printouts containing confidential medical information on individuals might be left unsecured.

Monterey County is a self-insured employer and is a "covered entity" under the Act.

The Final Rules regarding this federal act were published in the Federal Register (45 CFR Parts 160, 162 and 164 Health Insurance Reform, and Final Rules). Covered entities, such as Monterey County, have certain duties pursuant to HIPAA, including the duty to maintain the privacy of health information records that have information on them that link them to the patient they concern. Basically, when you have these two elements: a) a medical record, and b) identifying information which identifies who the medical record pertains to, then you have a "privacy record" under HIPAA. These types of records are also known as "Protected Health Information" (PHI). There are requirements under the Act that call on covered entities to give notice to parties (patients who are the subject of PHI) about the entity's privacy practices, legal duties, and the patient's rights concerning their health information.

BASIC RULES to CONTROL PHI

When health information that qualifies as PHI is received by our department, it will be kept only in one of the following locations:

1. The official D.A. file, if related to a filed case. (or in the case of a rejected case with that stored rejected case).
2. The official investigation file of the D.A. Investigator (if any) assigned to the case.
3. The official Victim of Crime file (if any) located within the Victim/Witness Assistance Unit.
4. District Attorney's Office employee health information will be kept only in the employee medical files, which are under the control of the department Benefits Coordinator.

5. Back-up copies of employee PHI information related to a worker's compensation claim may also be kept in the locked file cabinet of the individual supervisor who is monitoring a worker's compensation case involving an employee.

If PHI (Protected Health Information) is received electronically by anyone in our department, the recipient should do the following with that PHI:

a) Save it to a CD specifically labeled with the D.A. case number and "PHI". That CD is then to be placed in the D.A file, or;
b) The report or data electronically received may be printed onto paper and that paper copy placed in the official D.A. investigator file, official victim file or official D.A. file.
c) The electronically stored version should then be the deleted from the receiving computer.

TECHNICAL SAFEGUARDS

At no time will an individual's PHI medical information be left on a computer hard drive or on the e-mail system of a computer. Upon copying the information for the D.A. file, the official victim unit file, or D.A. Investigator's file, the electronic version will always be deleted.

PHYSICAL SAFEGUARDS

The District Attorney's Offices where its D.A. files and investigation files are stored will be locked at night when all employees and County employed janitors have left the premise.

Additionally, the District Attorney's Office will ensure that all D.A. files stored by "offsite" vendors are similarly protected and that when they are disposed of, that they are disposed of in such a manner that the PHI in the files cannot be used or identified by anyone who may come across them.

The District Attorney's Supervising Investigators will ensure that all D.A. rented and free locked storage spaces where PHI documents might be stored in D.A. files or D.A. investigative files, are locked and secured when not occupied by D.A. employees. The D.A. Supervising Investigators will be responsible for the proper destruction of any such stored file containing PHI. Individual investigators storing files with PHI will be sure that the PHI is destroyed or returned to the patient when the file (and its PHI content) is no longer needed by them for official purposes.

The Supervisor of the Victim/Witness Assistance Unit shall see that the "Victim of Crime Files" containing PHI are secured at night and that the files containing PHI are disposed of properly when no longer needed.

ADMINISTRATIVE SAFEGUARDS

The District Attorney, his administrative staff, and the County of Monterey have a duty to keep employees trained in regard to this policy and the procedures used to maintain the integrity of this policy. The responsibility for scheduling this training for the D.A. staff will fall to the department's Benefits Coordinator.

The department's Benefits Coordinator is assigned to attend County meetings on HIPAA and keep the District Attorney informed of County recommendations in regard to the policy.

BREECHES OF PRIVACY POLICY

Any employee of the District Attorney's Office who becomes aware of any breech of privacy regarding PHI under the Act or this policy is to report it immediately to their supervisor, so that remedial steps can be taken to correct the situation.

Managers and Supervisors who become aware of any breech of privacy are required to notify Monterey County Risk Management and the designated County Compliance and Security Officer of the breech within two working days.

Employees of this department who fail to follow the rules of this policy are subject to disciplinary action, up to and including termination from employment. If employees have specific questions about this policy, they should direct those questions to the District Attorney, in writing, through their supervisor.