

HIPAA-Security for ALL Consumers

Health Insurance Reform and Security Standards were developed and are highlighted by the Health Insurance Portability & Accountability Act (HIPAA). The rule adopts the standards for the *security of electronic protected health information to be implemented* by health plans, health care clearing houses and certain health care providers.

The use of the security standards are intended to improve Federal and Private Health programs and the effectiveness and efficiency of the health care industry in general by establishing a level of protection for certain electronic health information. The standards are comprehensive, scalable (effectively cover all size entities) and are not linked to specific technology.

Regulations have been in effect since April 21, 2003 and the deadline for compliance is April 2005 for large health plans and health care clearing houses and April 2006 for small entities.

Section 1173d of the Act provides that, “covered entities that maintain or transmit health information are *required to maintain reasonable and appropriate administrative, physical and technical safeguards to ensure the integrity and confidentiality of the information and to protect against any reasonably anticipated threats, such as unauthorized use or disclosure.*”

The statute requires the privacy standards to cover individually identifiable health information. ANY electronic protected health information received, created, maintained or transmitted by a covered entity is covered by the rule. In particular, software programmable computers such as PC's, mini-computers and mainframes must be protected.

There are four categories of requirements to safeguard the integrity, confidentiality and availability of the records: Administrative Procedure, **Physical Safeguards**, Technical Services, and Technical Mechanisms.

Physical Safeguards are security measures to protect a covered entity's electronic information system and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion. The implementation specifications are Contingency Operations, Facility Security Plan, Access Control and Validation Procedures and maintenance records.

Section 164.312 includes standards regarding access controls, audit controls, integrity and transmission security. Of particular interest, in the Access Control section it is clearly stated “we require unique user identification...” and “use of any appropriate access control mechanism is allowed” in addition under Audit Control, “mechanisms must be put in place to record and examine activity.”

The intent of the Act is clear. The nearly eighty pages of text boils down to: *protecting personal information is a mandatory responsibility of the health care provider.* Access to the room or rooms with computers hosting the defined information must be protected with considerations for physical security, access control and audit capability. Protecting individual computers with electronic log-on devices or preventing physical removal via mechanical hardware also seems appropriate for most applications.

This is an unprecedented opportunity to increase the security of consumers.

