



Dear Clients and Friends,

HIPAA is one of the most complex and multi-layered laws that employers must grapple with. The security rules are the latest in a long line of HIPAA rules that started with the relatively easy to grasp concept of portability of insurance.

The most obvious concern regarding protected health information is disclosure or theft of data. Web site penetration, data hackers and misdirected information should be considered

and steps taken to reduce the risks of these types of disclosure.

Employers need to review their internal security measures. If computers are used by multiple employees – what procedures or documentation exists to determine who may have released information in error, for example?

*Sincerely yours,
Jim Lill, President*

HIPAA Deadline Looms

HIPAA's security rules apply to small health plans as of April 20, 2006. Small health plans are defined as plans with annual receipts of \$5 million or less. For insured plans, receipts would equate to premiums paid in the prior year.

Many employers may not realize that they have obligations under the HIPAA security rules. But, if they have a health plan steps should be taken to, at a minimum, assess the use of electronic protected health information (e-PHI) and the risk of inadvertent disclosure of e-PHI.

The federal rules provide general requirements for security standards.

"Covered entities must do the following:

- (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.

(4) Ensure compliance with this rule by its workforce."

In drafting the rules, regulators recognized that covered entities would have a wide range of technical sophistication. Therefore, the rules allow for flexibility in meeting many of the requirements. Key factors to consider in implementing the rules are the costs to comply, the risks of disclosure of e-PHI and the reasonableness of actions taken.

Employers with health plans should conduct a security risk assessment. This should include evaluating when PHI is transmitted electronically. Plan documents may also be revised to reduce some of the information subject to the rule.

Ask us about free COBRA and FSA administration!