March 25, 2005

HIPAA Security – Compliance Reminder

Just when you thought it was safe to say "HIPAA" again, HIPAA security compliance is upon us. If you have been following HIPAA privacy, you know that security is the latest, and hopefully last, piece of the HIPAA puzzle. Most covered entities covered the topic of security in their privacy policies in a very general way as the Department of Health and Human Services' final security regulations were issued in the same month as the privacy rules became effective for health care providers and large health plans.

Fortunately, HHS gave some time for covered entities to digest the new requirements and plan for compliance. The deadline for compliance is very similar to privacy in that for health plans HHS created two deadlines: April 20, 2005 for large health plans and April 20, 2006 for small health plans. Health care providers must be in compliance by April 20, 2005.

The new HIPAA security regulations require covered entities to take steps to protect the integrity, confidentiality and availability of protected health information that is transmitted or maintained in an electronic form, known as electronic protected health information or EPHI. The regulations provide for a very structured analysis of how covered entities would do this. Three separate areas of "safeguards" are to be looked at – administrative, physical and technical. Each of these safeguards has a number of standards that describe the particular security issues to examine and, in turn, each of the standards may have discreet "implementation specifications" that further breaks down the analysis.

As a result, every covered entity is going to ask itself the same questions. The answers, however, and as a result the security approach, will vary from covered entity to covered entity. This is because the security regulations do not dictate any particular method of security protection. The outcome the covered entity selects must be appropriate based on its size, its complexity and its capabilities. Also, a covered entity may consider things like its technical infrastructure, hardware, software and security capabilities. All these things must reflect a balance of the costs of a certain safeguard with the probability of a security incident occurring and the criticality of such an incident if it were to occur. Thus, there is no readily available "off the shelf" answer for HIPAA security.

After this self-examination and the decisions are made, the balancing considerations and the outcomes must be reflected in written security policies and procedures for the covered entity. These policies and procedures will tend to be a separate document from that created for HIPAA privacy compliance. Like HIPAA privacy, the covered entity's workforce must be trained on its security procedures, the plan documents must be amended and the business associate contracts must reflect compliance with security. Finally, a security official must be appointed who is responsible for compliance by the covered entity. The person could, but does not need to, be the same person as the privacy official.

If you have any questions concerning HIPAA security compliance, please contact the Seyfarth Shaw LLP Employee Benefits Group attorney with whom you work or any Employee Benefits Group Attorney on the website at www.seyfarth.com.