ALERT

HIPAA UPDATE FOR EMPLOYERS

April 17, 2006

If you are providing group health coverage to your employees – including major medical coverage or even a health flexible spending account – you need to pay attention to the HIPAA Electronic Security Regulations, the HIPAA Medical Privacy Regulations, and the HIPAA Portability Regulations. Subject to some very narrow exceptions, *all* employer-sponsored group health plans are now required to comply with these HIPAA regulations and other guidance from the government.

For instance, even though the April 14, 2004, deadline for complying with the HIPAA Medical Privacy Regulations has passed, it is still important to bring your company into compliance or to maintain your company's compliance despite continuing developments in medical privacy. In addition, employers should be aware that the Department of Health and Human Services (HHS) has provided guidance on how HIPAA medical privacy applies in an emergency situation, such as Hurricane Katrina. The HHS Bulletin on HIPAA Privacy and Disclosures in Emergency Situations can be downloaded at: http://www.hhs.gov/ocr/hipaa/KATRINAnHIPAA.pdf.

The enclosed Memorandum passes along some new information about HIPAA while also providing the answers to a number of "frequently asked questions". In particular, it covers the following:

- **HIPAA Electronic Security.** The deadline for complying with the HIPAA electronic security regulations is **April 20, 2006**, for most group health plans (i.e., those with less than $5 million in premiums). The focus of these rules is on protecting certain health information that is being exchanged *electronically* from unauthorized disclosure. Fortunately, many of the HIPAA electronic security rules are very similar to the medical privacy rules (e.g., sanctions, training, policies and procedures, business associate contracts, etc.) that have already been implemented by employers with group health plans. Other rules dovetail so that steps that have been taken for privacy compliance can form the basis for security compliance. Consequently, most employers will find compliance with electronic security less burdensome than compliance with HIPAA medical privacy.

- **HIPAA Portability.** The deadline for complying with the HIPAA portability regulations has passed. However, it is still important to bring your company into compliance or to maintain your company's compliance by issuing the Notice of HIPAA Special Enrollment Rights and Notice of Preexisting Condition Exclusion.

If you have any questions about any of these developments or would like to discuss any of these topics in further detail, please feel free to call Eric Namee or Steven Smith at (316) 267-2000.

The 2005-2006 edition of The Hinkle Elkouri HIPAA Handbook is now available and provides high-level explanations in "plain English", along with ready-to-use compliance checklists and forms, for HIPAA electronic security and medical privacy. *Please see the enclosed information sheet and order form for more details.*

HINKLE ELKOURI
LAW FIRM L.L.C.

Downtown Office 2000 Epic Center • 301 North Main Street, Wichita, KS 67202
East Office 8621 East 21st Street North, Suite 200, Wichita, KS 67206
(316) 267-2000 • www.hinklaw.com

April 17, 2006

MEMORANDUM

Re: An Update for Employers on Developments Related to HIPAA

I. DEADLINE TO COMPLY WITH HIPAA ELECTRONIC SECURITY RULES IS APPROACHING

The April 20, 2006, deadline to comply with the HIPAA electronic security rules is quickly approaching. The HIPAA security rules require that safeguards be put in place to protect the confidentiality, integrity, and availability of electronic "protected health information" (or "PHI"). The security rules, like the HIPAA medical privacy rules, apply to "covered entities." This term includes health plans, clearinghouses, and most health care providers. Employers will not normally be "covered entities" under the HIPAA security rules (unless the employer, for example, happens to be a doctor's office or an insurance company), but employers, as plan sponsors, must agree to comply with the security requirements in order to receive certain health information from their group health plans.

Employers with group health plans subject to the electronic security rules should do the following on or before April 20, 2006:

- **Continue the security measures required by the HIPAA privacy rule.** The HIPAA privacy rule requires appropriate technical safeguards to be in place. For example, rooms and cabinets where PHI may be found should be locked; electronic files containing PHI should be password protected; and policies and procedures regarding computer workstation use and the transmission of PHI by electronic means should be in place. Employers should continue these security measures under the electronic security rules.

- **Appoint a Security Officer.** Just as the privacy rules required the appointment of a privacy officer and contact person to manage compliance with the privacy rules, the security rules require the appointment of a security officer. The responsibility for the security rules will rest with this individual. The designation of this position, the duties and responsibilities associated with this person, and the acceptance of this position by the appointed individual should be well documented.

- **Risk Analysis.** Under the HIPAA electronic security rules, the use, transmission and maintenance of all electronic PHI should be assessed. A risk analysis should then be performed to identify the potential risks of improper disclosure, the potential risks to confidentiality, and the vulnerability of PHI maintained or transmitted in the group health plan's databases. All risks, including those stemming from human error and those resulting from malicious activity, must be examined. Once the risk analysis is completed, it should be well documented and any discovered risks and vulnerabilities should be addressed.

Downtown Office 2000 Epic Center • 301 North Main Street • Wichita, KS 67202-4820 • (316) 267-2000 • Fax (316) 264-1518
East Office 8621 East 21st Street North • Wichita, KS 67206 • (316) 267-2000 • Fax (316) 630-8375
www.hinklaw.com

- **Policies and Procedures.** Employers will also need to build on the policies and procedures that were implemented under the medical privacy rules. The updated policies and procedures should cover the access and control of electronic PHI.

- **Business Associate Agreements.** The electronic security rules require that business associate agreements include language protecting electronic PHI. Consequently, if a business associate handles electronic PHI, employers will need to amend the current agreements between their group health plans and their business associates for the security rules.

- **Plan Document Amendments.** Finally, in order for electronic PHI to be created, received, maintained or transmitted by the employer-plan sponsor, the plan document will need to be amended. There are not, however, any required changes to the summary plan description. If we prepared your group health plan documents, you should have received an engagement letter from us regarding amending your plans for HIPAA electronic security. If you have engaged us to prepare your amendments, you will be receiving the appropriate amendments shortly.

II. **Required Notices under the HIPAA Portability Rules**

Final HIPAA portability rules went into effect on July 1, 2005. These rules require almost all group health plans to issue two notices. The rules, however, do not establish notice requirements for health flexible spending accounts and other group health plans that are considered "limited benefits" under HIPAA.

There are two ways that a group health plan may be a "limited benefit" and thus exempt from the notice requirements. First, if the benefits are provided under a separate policy, certificate, or contract of insurance, then they may be "limited benefits." Second, if the benefits are not an "integral" part of a group health plan, then they may be "limited benefits." A benefit is not an "integral" part of a group health plan (1) if the participant has a right not to elect coverage, or, (2) if the participant does elect to receive coverage, the participant must pay an additional premium or contribution for it.

Both limited-scope dental and vision benefits may be "limited benefits" and excepted from the HIPAA portability rules. Limited-scope dental benefits are defined as "benefits substantially all of which are for the treatment of the mouth" and limited-scope vision benefits are defined as "benefits substantially all of which are for treatment of the eye." These benefits may be "limited benefits" if they are either provided under a separate policy, certificate, or contract or insurance, *or*, they are not "integral" to the major medical coverage (regardless of whether they are stand-alone plans or bundled with major medical coverage).

Although many insurance companies may be providing these notices to potential enrollees on the employer's behalf, this responsibility ultimately resides with the employer. Consequently, you should determine whether or not your insurance company is providing these notices on your behalf. ***If it is not, please feel free to contact us and we will be happy to provide you with the appropriate notices.***

The two required notices are as follows:

- **Notice of HIPAA Special Enrollment Rights.** As a general rule, if an employee declines coverage for him- or herself and/or any dependents, they may not have the opportunity to enroll in the plan again until the next open enrollment period. Under certain circumstances, however, a plan must allow the employee and/or any dependents to enroll mid-year.

  For example, if an individual declines coverage because he or she has other health coverage and the individual subsequently loses such other coverage, the plan must permit the individual to enroll mid-year. The individual, however, must exercise this "special enrollment right" within 30 days of the loss of coverage. Similarly, if an employee gains a dependent through marriage, birth, adoption or placement for adoption, the employee and his or her dependents must be permitted to enroll in the plan mid-year. Again, this request must be made within 30 days after the marriage, birth, adoption or placement for adoption.

  The Notice of HIPAA Special Enrollment Rights informs potential enrollees of the above special rights. In particular, this Notice must be given to *employees* who are potential enrollees; it is not, however, necessary to give this notice directly to a dependent. If you have a calendar year plan, you should have provided this Notice to eligible employees of the applicable group health plans on or before January 1, 2006. If you do *not* have a calendar year plan, this Notice should have been distributed on or before the plan year first beginning after July 1, 2005.

- **Notice of Preexisting Condition Exclusion.** Some, but not all, plans impose what is known as a "preexisting condition exclusion." This means that if an individual has a medical condition for which medical advice, diagnosis, care, or treatment was recommended or received within the preceding 6-month period, the individual has to wait a certain period of time before the plan will provide coverage for the condition. This exclusion may last up to 12 months for those who enroll when first eligible or up to 18 months for "late" enrollees. The length of this exclusion period, however, may be reduced by the number of days that the enrollee had prior creditable health coverage.

  The Notice of Preexisting Condition Exclusion explains what it means for the individual and the plan to have a preexisting condition exclusion. If your plan is a calendar year plan and has a preexisting condition exclusion, this Notice should have been distributed on or before January 1, 2006 to all employees who were eligible to enroll. If your plan is *not* a calendar year plan, but does have a preexisting condition exclusion, this Notice should have been distributed on or before the first plan year that begins after July 1, 2005.

  If your plan does not have a preexisting condition exclusion, this Notice is not necessary. However, you should examine your plans carefully and be wary of "hidden" preexisting condition exclusions. For example, you may have a dental plan (to which the above described exception from the HIPAA requirements does not apply) which excludes coverage for dental injuries unless the injury incurred while the person was covered under the plan. This would qualify as a preexisting condition exclusion and obligate you, as the employer, to send out a Notice of Preexisting Condition Exclusion.

In sum, the above two Notices should be distributed to all *potential* enrollees who are employees. This means that the plan should provide this notice at or before the time the employee is initially offered the opportunity to enroll. If the plan has a waiting period, we recommend that the

applicable notice(s) be included with the enrollment material so that the individual may make a more informed decision regarding his or her enrollment in the plan.

If you are a client of our firm who has missed the deadlines, you should contact us immediately and we will provide you with the appropriate Notices as well as advice on distributing them in a manner that minimizes your legal exposure.

CONCLUSION

HIPAA electronic security and portability are complicated sets of regulations. Now that the rules are effective for all covered entities, we hope that the Department of Health and Human Services will continue to provide us with additional guidance on following the rules. The purpose of this Memorandum is to provide you with an update on developments in HIPAA electronic security and portability that may be of interest to you as an employer. It is not a comprehensive analysis or a list of every development that has taken place. If you have any questions about any of the topics discussed in this Alert, please feel free to call Eric Namee or Steven Smith at (316) 267-2000.

THE HINKLE ELKOURI HIPAA HANDBOOK

We have updated The Hinkle Elkouri HIPAA Handbook to reflect changes in HIPAA medical privacy, and electronic security. Our purpose in writing The HIPAA Handbook is to help employers understand how to comply with HIPAA. It provides high-level explanations in "plain English", along with ready-to-use compliance checklists and forms. *For more details, please see the enclosed information sheet and order form.*