ALERT

HIPAA PRIVACY FOR EMPLOYERS HAS CHANGED. IMMEDIATE ACTION IS REQUIRED.

November 20, 2009

The American Recovery and Reinvestment Act of 2009 ("ARRA") – also known as the "Economic Stimulus Bill" – made important changes to the HIPAA Medical Privacy and Security Rules. *If you offer a health flexible spending account or other self-funded group health plan coverage (e.g., medical, dental, vision, or prescription drug benefits), these changes affect you – and there are steps you are legally required to take. In addition, if you offer fully insured group health benefits to employees and have access (or would like to have access) to "protected health information" ("PHI") from your plan, there are also steps that you are legally required to take.*

These changes, and the steps you are required to take, are summarized in more detail in the attached memorandum. The four primary changes to HIPAA coming out of ARRA are as follows:

- **New rules and requirements if there is an unauthorized use or disclosure of PHI (referred to as "Breach Notification Rules");**
- **Expansion of certain individual rights;**
- **Expanded requirements for business associates; and**
- **Strengthened enforcement of HIPAA and increased penalties.**

Some of these changes have already taken effect; other changes will take effect shortly. To comply with these new HIPAA privacy rules, and as explained in more detail in the attached memorandum, employers who sponsor group health plans for their employees will need to take the following steps (among others):

(1) Understand the breach notification rules so that you will recognize when there has been an impermissible use or disclosure of PHI under the HIPAA Medical Privacy and Security Rules and notify the appropriate parties accordingly;

(2) Update group health plan documents as necessary;

(3) Revise HIPAA policies and procedures to reflect the breach notification requirements, the change to individual rights, and documentation provisions;

(4) Update your HIPAA Privacy Notice;

(5) Train employees who may have access to PHI on the new rules; and

(6) Update business associate agreements.

This represents a very brief summary of some very complicated statutory and regulatory provisions. Because of the very short time frame for compliance, and because of the potentially serious consequences of noncompliance, ***it is important for you or someone in your organization to read the attached memorandum.*** If you have questions regarding the HIPAA medical privacy and security changes in ARRA and the regulations thereunder, please feel free to call Ruhe Rutter or Steven Smith at (316) 267-2000.

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

HINKLE ELKOURI
LAW FIRM L.L.C.

MEMORANDUM

HIPAA PRIVACY FOR EMPLOYERS HAS CHANGED. IMMEDIATE ACTION IS REQUIRED.

The American Recovery and Reinvestment Act of 2009 ("ARRA") – also known as the "Economic Stimulus Bill" – made important changes to the HIPAA Medical Privacy and Security Rules. This Memorandum is intended to address how the HIPAA privacy changes in ARRA affect employers who offer group health plans to their employees. This Memorandum is not intended to address any changes that may affect doctors and other health care providers.

The four primary changes to HIPAA medical privacy coming out of ARRA, and discussed in this Memorandum, are:

- New rules and requirements if there is an unauthorized use or disclosure of PHI (referred to as "Breach Notification Rules");
- Expansion of certain individual rights;
- Expanded requirements for business associates; and
- Strengthened enforcement of HIPAA and increased penalties.

If you offer a health flexible spending account or other self-funded group health plan coverage (e.g., medical, dental, vision, or prescription drug benefits), these changes affect you – and there are steps you are legally required to take. In addition, if you offer fully insured group health benefits to employees and have access (or would like to have access) to "protected health information" from your plan, there are also steps that you are legally required to take.

Note: If you have a health flexible spending account, your plan is subject to HIPAA medical privacy and security compliance (even if your access to protected health information is very limited), unless you have fewer than 50 eligible employees *and* you self-administer the plan.

I. – What's Going On

To understand the changes that Congress has made, we need to provide some background information. The basic principle underlying HIPAA medical privacy is this: *information about your health should be private and that information should not be used or disclosed by anyone for any purpose except when that information is needed to provide medical care or to process and pay claims for your medical care.* There are some additional exceptions to sharing health information, such as exceptions if information is needed for law enforcement purposes or if you have given permission for the information to be used or disclosed, but this is the general principle underlying HIPAA medical privacy.

To implement this fairly simple principle, the government has issued many lengthy and complicated regulations, including the following:

- The HIPAA **Medical Privacy** Regulations tell us, in considerable detail, what information is considered to be "protected health information" (or "PHI"), who is allowed to see and use PHI, and when they are allowed to do so. Generally, these regulations apply only directly to "covered entities," such as medical

providers and group health plans. Having said that, however, if you, the employer, have access (or would like to have access) to PHI through your group health plan, then you are considered responsible for the HIPAA compliance rules that your group health plan must follow and must act on behalf of your group health plan.

In this Memorandum, we are addressing the HIPAA privacy rules for *employers*, not doctors. Therefore, we have only focused on the rules' application to group health plans for which employers are responsible and we have not focused on other "covered entities," such as doctors. Consequently, we have tried to avoid the use of the term "covered entity" and use the term "group health plan" instead.

- The HIPAA **Security Regulations** tell us, also in considerable detail, what steps have to be taken to make sure that electronic PHI is not disclosed to anyone who is not authorized to see PHI. These regulations apply to group health plans and, as a result of the ARRA amendments, most of the security requirements apply to "business associates" as well.

- The HIPAA **Breach Regulations** tell us, again in considerable detail, what steps have to be taken if PHI is accessed by someone who is not authorized to see PHI under the Medical Privacy and Security Regulations. These regulations are new.

II. – New Breach Notification Rules

The new breach notification rules essentially require employers, who are acting on behalf of their group health plans, to notify certain parties of any "breach" of PHI, i.e., the "unauthorized acquisition, access or use or disclosure of [unsecured PHI] which compromises the security or privacy of such information."

In particular, under ARRA, *group health plans* have significant new notification obligations when they discover (or, through "reasonable diligence," should have discovered) a "breach," resulting in the disclosure of "unsecured PHI." Keep in mind that "unsecured PHI" is any PHI that has not been encrypted or destroyed. If the PHI is properly encrypted or destroyed in accordance with the Department of Health and Human Service ("HHS") regulations, then it is "secured PHI." PHI that is "secured" is not subject to these breach rules. Because destruction or encryption of all PHI is not always a viable option for group health plans, however, group health plans (and most business associates providing services on their behalf) will usually have some sort of "unsecured PHI" and, therefore, must ensure compliance with the new breach notification rules. For example, if a report containing PHI has been printed, the printed copy will have PHI and such PHI will be considered "unsecured."

Determination if a Breach has Occurred. The following three-step approach should be used by a group health plan to determine if a breach has occurred:

(1) Determine whether there has been an impermissible use or disclosure of PHI under the HIPAA Medical Privacy and Security Rules;

(2) Determine whether such impermissible use or disclosure compromises the security or privacy of the PHI – that is, if it poses a significant risk of financial, reputational, or other harm to the individual – and document the risk assessment performed in making this determination; and

(3) Determine whether the incident falls within one of three limited exceptions to the definition of a "breach." *For example*, an unintentional disclosure of PHI by someone authorized to access PHI to another authorized individual, if done in good faith and within the person's scope of authority but does not result in further impermissible use or disclosure of the PHI would not be a "breach."

It is the group health plan's obligation to determine whether a breach has occurred. Therefore, employers who sponsor group health plans who access, or could potentially access, PHI need to formalize their risk assessment processes and procedures and document their breach determinations.

Required Notifications. If a group health plan determines that a breach has occurred, then it will be required to comply with the new breach notification rules. The following is intended to be a very brief summary of those rules:

(1) **Notification to Individuals.** Written notice to affected individuals must generally be given by first-class mail. The notice must include certain information. Notice must be provided by the group health plan "without unreasonable delay" – but in no case later than 60 days – after discovery of a breach of "unsecured PHI".

(2) **Notification to Media.** If the PHI of 500 or more individuals in a single State or jurisdiction is involved in the breach, notice must also be given to prominent local media outlets within the timeframe stated in (1), above.

(3) **Notification to HHS.** If the PHI of 500 or more individuals is involved in the breach, HHS must be notified at the same time as individual notice is provided. If the PHI of less than 500 individuals is involved in the breach, the group health plan must maintain a log and submit it annually to HHS (within 60 days after the end of the calendar year).

Other Administrative Requirements. In addition, employers acting on behalf of their group health plans are required to do the following in light of the new breach notification rules:

(1) Revise HIPAA policies and procedures to reflect the notification requirements;

(2) Train workforce members to secure PHI, if applicable, and to promptly notify the group health plan if the privacy or security of "unsecured PHI" has been breached;

(3) Sanction workforce members who violate the notification requirements; and

(4) Retain documentation related to the notification requirements for six years.

Application to Business Associates. Although most of the new breach notification rules apply to "covered entities," such as group health plans, business associates are also directly affected by these rules. The new rules require business associates to notify group health plans of any breach of "unsecured PHI" without unreasonable delay, but in no case later than 60 days after the breach is discovered. The effect of this rule on business associate agreements is briefly addressed in Part IV of this Memorandum.

Effective Date. The breach notification rules became effective September 23, 2009. Because of the short time frame given to comply with these rules – the regulations were not published until August 24, 2009 – HHS will not enforce sanctions for failure to provide the notifications until **February 22, 2010**. Group health plans, however, are expected to comply now and should begin compliance efforts as soon as possible.

III. – Expansion of Certain Individual Rights

The right to request restrictions on PHI and the right to an accounting of PHI have been modified by ARRA. Prior to ARRA, individuals had the right to request restrictions on the use or disclosure of their PHI. "Covered entities" (e.g., health care providers, group health plans), however, were *not* required to comply with the restrictions. Under ARRA, "covered entities" *are required* to honor an individual's request to restrict the disclosure of PHI when the following is true:

(1) The disclosure is to a group health plan for purposes of payment or health care operations (not treatment); *and*

(2) The PHI pertains solely to a health care item or service for which the provider has been paid by the individual, out-of-pocket, in full.

In addition, prior to ARRA, individuals had the right to request an accounting (of up to six prior years) of certain disclosures of their PHI, but such accounting did not have to include disclosures for purposes of treatment, payment, or health care operations. Under ARRA, the accounting, if requested, must now include any disclosure for purposes of treatment, payment, or health care operations if such disclosure involves an *electronic record* of health-related information on the individual that is created, gathered, managed, and consulted by authorized healthcare clinicians and staff. This type of accounting need only date back three years instead of six years. A group health plan can have electronic health records if such records are consulted or managed by health care staff working for the plan who perform activities such as utilization review and disease management.

Although the enhancement to these individual rights will primarily affect health care providers, these requirements technically apply to group health plans as well. Consequently, plan documents, policies and procedures, and the HIPAA privacy notice, should be updated accordingly.

IV. – Expanded Requirements for Business Associates

Business associates are third parties (e.g., insurance brokers, consultants, third-party administrators, attorneys) that assist group health plans in performing a function or activity or that provide certain services involving the use or disclosure of PHI.

The HIPAA Medical Privacy and Security Rules permit a group health plan to disclose PHI to a business associate, or allow a business associate to create or receive PHI on behalf of a group health plan, but *only if the group health plan obtains satisfactory assurances that a business associate will appropriately safeguard the information*. The HIPAA Medical Privacy and Security Rules further require that the assurances be documented in a written contract or other agreement that satisfies HIPAA's requirements. Further, under the HIPAA Medical Privacy Rule, *the business associate agreement must establish the permitted use and disclosures of PHI by the business associate*. With certain limited exceptions, this means that the business associate may not be allowed to use or disclose PHI *in any way that the group health plan could not use or disclose it.*

Why are we telling you this? Up until now, business associates have only been contractually obligated to group health plans to safeguard PHI through a business associate agreement. Effective February 17, 2010, most HIPAA security requirements and some HIPAA privacy requirements will apply *directly* to business associates. However, because a group health plan cannot share PHI with its business associate unless it receives adequate assurances (through a business associate agreement) that the business associate will properly safeguard PHI, business associate agreements must be updated to reflect the new obligations on business associates that affect their relationship with the plan. This generally means updating business associate agreements for the new individual rights described in Part III of this Memorandum and for the breach notification obligation which applies directly to business associates, described in Part II of this Memorandum. In addition, a business associate agreement could, if both parties agree, require the business associate to make some or all of the notifications to individuals, the media, and/or HHS that are required by "covered entities" and that are briefly described in Part II of this Memorandum.

V. – Strengthened Enforcement of HIPAA under ARRA

Under the ARRA amendments to the HIPAA Medical Privacy and Security Rules, it is expected that there will be a marked shift toward greater HIPAA enforcement. This is due to the following changes brought by ARRA:

(1) Civil monetary penalties for HIPAA violations have increased significantly. Prior to ARRA, the maximum penalty was $100 for each violation and up to $25,000 for similar violations in the same year. After ARRA, penalties range from $100 to $50,000 for each violation with caps on the total penalty amount for similar violations in the same year. The penalty may vary depending on the degree of culpability (i.e., no knowledge, reasonable cause, and willful neglect) as follows:

(a) Where there is no knowledge of a violation (or no possibility of having known of a violation after exercising "reasonable diligence"), the penalty will be between $100 and $50,000 per violation, but the total penalty for all "identical" violations for that calendar year will not exceed $1,500,000.

(b) Where the violation is due to "reasonable cause" and not to willful neglect, the penalty will be between $1,000 and $50,000 for each violation, but the total penalty for all "identical" violations for that calendar year will not exceed $1,500,000.

(c) Where the violation is due to willful neglect, but is corrected within 30 days of the "covered entity" becoming aware of the violation, the penalty will be between $10,000 and $50,000 for each violation, but the total penalty for all "identical" violations for that calendar year will not exceed $1,500,000.

(d) Where the violation is due to willful neglect and it is not corrected within 30 days of the "covered entity's" knowledge of the occurrence of the violation, the penalty will be at least $50,000 for each violation with the total penalty for all "identical" violations for that calendar year not to exceed $1,500,000.

These new penalty provisions are already in place.

(2) Beginning two years after the enactment of ARRA – that is, beginning in February 2011 – HHS is required to formally investigate any complaint where a preliminary investigation indicates a possible violation of the Privacy and Security Rules due to willful neglect. If a violation is found and the violation was due to willful neglect, HHS will be *required* to impose a penalty.

(3) State attorneys general have now been given the power to enforce the law. This is a significant change because it creates some uncertainty as to how the law will be enforced. If HHS enforces HIPAA, how HIPAA will be interpreted and enforced may be more predictable because HHS itself wrote the regulations on HIPAA medical privacy and security and one of its primary areas of oversight is HIPAA. A state attorney general, however, must focus on the enforcement of a wide variety of laws (not just HIPAA) and may interpret or enforce the law differently than what one might expect from career professionals at HHS who are experts on HIPAA.

(4) Any penalties or settlements collected for privacy and security violations must go to HHS for enforcement purposes (as opposed to pre-ARRA law where the money went to the general treasury). *However, individuals harmed by the violation(s) are entitled to a percentage of the penalty or monetary settlement collected by HHS.* This may provide incentive for individuals to file HIPAA complaints. These enforcement provisions are effective in 2011. The percentage to which individuals will be entitled will be set forth in future regulations.

VI. – Steps to be Taken

In light of the ARRA amendments to the HIPAA Medical Privacy Rules that are summarized above, employers will need to understand the changes and take the following steps:

(1) **Update Plan Documents.** If you have self-funded group health plan(s) or have access (or would like to have access) to PHI from your fully insured group health plan(s), you will need to update your plan documents to reflect changes made by ARRA. If we prepared HIPAA medical privacy provisions for your plan documents, we will be contacting you and providing you with updated language.

(2) **Update HIPAA Policies and Procedures.** If your plan(s) are set up to receive PHI (i.e., they have the appropriate HIPAA provisions referred to in (1) above), you will need to update your HIPAA policies and procedures to address the enhanced individual rights and the new breach notification requirements. You will also need to update policies and procedures on various documentation provisions, such as documentation of breaches, and on HIPAA training for workforce members regarding the security of PHI and notifying proper parties of breaches.

(3) **Privacy Notice.** If your plan(s) are set up to receive PHI, you will need to update your HIPAA privacy notice to reflect the enhanced individual rights under ARRA.

(4) **Update Business Associate Agreements.** You will need to update all business associate agreements that you have with any business associates.

****

This Memorandum represents a very brief summary of some very complicated statutory and regulatory provisions. Because of the very short time frame for compliance, and because of the potentially serious consequences of noncompliance, ***it is important for you or someone in your organization to ensure that your group health plans, business associate agreements, and HIPAA medical privacy and security policies, procedures, and other documents are up to date.*** If you have questions regarding the HIPAA medical privacy and security changes in ARRA and the regulations thereunder, please feel free to call Ruhe Rutter or Steven Smith at (316) 267-2000.