HINKLE LAW FIRM LLC
hinklaw.com 316.267.2000

July 10, 2013

HIPAA Update for Employers: Action Required by September 23rd

While we have all been focused on Health Care Reform, the government has also been active on other fronts affecting employer-provided medical benefits. If you are providing group health coverage to your employees – including major medical coverage or even a health flexible spending account – you also need to be aware of recent changes to the HIPAA Medical Privacy, Security, and Breach Notification regulations.

Subject to some very narrow exceptions, *all* employer-sponsored group health plans are required to comply with these HIPAA regulations and other guidance from the government. That means that 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 soon to comply with changes made to the HIPAA regulations. The same is true 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.

In 2009, the Department of Health and Human Services (**"HHS"**) issued interim regulations governing the HIPAA Medical Privacy, Security, Breach Notification, and Enforcement Rules. Many employers amended their group health plans and their policies and procedures in light of these interim regulations. Then, earlier this year, HHS issued the long-awaited final regulations, which replace the 2009 interim regulations. The deadline to comply with the new final regulations is **September 23, 2013**.

Key Changes

The following is a brief summary of the key changes made by the final regulations affecting employee benefit plans:

(1) **Expanded Definition of "Business Associate."** The final regulations expand the definition of "business associate" to include virtually all entities that create, maintain, receive, or transmit PHI when acting on behalf of a plan or another business associate. This includes subcontractors of a business associate (and subcontractors of subcontractors) that handle PHI – and so on, no matter how far downstream the PHI flows.

Plans and business associates, including subcontractors, will need to adopt new business associate agreements by the September 23, 2013 deadline. (The deadline is extended to September 22, 2014 for certain existing business associate agreements that meet specified requirements.) These new agreements must include provisions requiring the business associate to do the following:

DOWNTOWN WICHITA
301 N. Main St., Ste. 2000
Wichita, KS 67202-4820

EAST WICHITA
8621 E. 21st St. N., Ste. 200
Wichita, KS 67206-2991

OVERLAND PARK
6800 College Blvd., Ste. 600
Overland Park, KS 66211-1533

(a) Report any breach of unsecured PHI to the plan without "unreasonable delay" (and in no event later than 60 days after discovering the breach);

(b) Comply with the plan's HIPAA privacy obligations and with the HIPAA Privacy Rule;

(c) Enter into HIPAA-compliant business associate agreements with any subcontractors that handle PHI on behalf of the business associate; and

(d) Comply with the HIPAA Security Rule with respect to electronic PHI. This includes the adoption of administrative, physical, and technical safeguards.

(2) **Notice of Privacy Practices.** The final regulations require a plan to modify its Notice of Privacy Practices regarding uses and disclosures that require authorization. The Notice of Privacy Practices must include a statement that prior authorization is required for most uses and disclosures of psychotherapy notes, marketing disclosures, and sales of PHI. The Notice of Privacy Practices must also state that the individual has the right to be notified in the case of a breach of unsecured PHI. *HHS has clarified that, because these changes are "material," covered entities must distribute a new Notice of Privacy Practices to individuals by September 23, 2013.*

(3) **Modified Breach Definition.** The final regulations expand the definition of a "breach" to provide that any impermissible use or disclosure of PHI is ***presumed*** to be a breach, unless it is demonstrated that there is a ***low probability*** that PHI has been compromised. This is determined based on a four-part risk assessment test that considers the following factors:

(a) The nature and extent of the PHI involved in the breach;

(b) The unauthorized person who used the PHI or to whom the disclosure was made;

(c) Whether the PHI was actually acquired or viewed; and

(d) The extent to which the risk to PHI has been mitigated.

If the risk assessment fails to demonstrate that there is a low probability that PHI has been compromised, breach notification is mandatory.

Note: The 2009 interim regulations included a breach definition, and many employers amended their plan documents to reflect this standard. This old definition of "breach" continues to apply through September 22, 2013. Beginning on September 23, 2013, the new breach definition, set forth in the final regulations and discussed immediately above, will replace the old definition.

(4) **PHI after Death.** The final regulations slightly relax the restrictions on the disclosure of an individual's PHI after the individual's death. For example, PHI ceases to be PHI once 50 years have passed since the individual's death.

(5) **Individual Rights.** The final regulations expand an individual's right to receive electronic copies of his/her PHI and to restrict disclosures to a health plan with respect to treatment for which the individual has fully paid out-of-pocket.

(6) **HHS Investigations.** The final regulations require HHS to investigate any complaint or violation if a preliminary review of the facts indicates even a *possible* violation due to willful neglect.

(7) **Increased Penalties.** The final regulations substantially increase the potential civil monetary penalties for HIPAA violations from a penalty of "up to $100" per violation to a penalty of "$100 to $50,000" per violation. The amount of a penalty varies depending on the level of culpability, which ranges from "did not know" to "willful neglect." The penalty amount is capped at $1.5 million per year.

Steps Employers Need to Take

The impact of the final regulations on employers and employer-sponsored group health plans may be summarized as follows:

(1) For most plans, no changes to the plan documents appear to be necessary at this time. However, if you have a self-funded group health plan (including a health flexible spending account), and your plan documents were not updated for the 2009 interim regulations, they may need to be updated now.

(2) HIPAA Privacy Policies and Procedures must be updated. The regulations require employers to have HIPAA Privacy Policies and Procedures in place, so for employers that do not have them, now is a good time to adopt them.

(3) Update and redistribute the HIPAA Notice of Privacy Practices.

(4) Update any business associate agreements entered into by the plan. This may be the single most significant effect of the final regulations. Going forward, the plan administrator will need to begin using an updated business associate agreement, and existing business associate agreements will need to be amended.

****

This Alert represents a very brief summary of the new HIPAA final regulations. Because of the very short time frame for compliance, and because of the potentially serious consequences of noncompliance, ***it is very important for employers to ensure that their group health plans, business associate agreements, and HIPAA medical privacy and security policies, procedures, and other documents are up to date***.

Please note that if we previously prepared or assisted you with your HIPAA documents, we will be in contact with you shortly to help you comply with these new rules. If we did not prepare your HIPAA documents, and you have questions or would like our assistance, please feel free to call Eric Namee, Steven Smith, or Brad Schlozman at (316) 267-2000.

HINKLE
LAW FIRM LLC