BUTZEL LONG
ATTORNEYS AND COUNSELORS

Employee Benefits E-news

January 6, 2010

Deadline Approaching for Group Health Plan Compliance with HIPAA Privacy and Security Law Changes

In 2009, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules were amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act. HITECH imposed significant new requirements on employer group health plans and their business associates. Among other things, HITECH added security breach notice duties, expanded accounting for health record disclosures, increased penalties and enforcement, extended many HIPAA rules and penalties to business associates, clarified existing provisions, and required more specific guidance on various standards. Only employers with fully insured plans which do not create or receive protected health information (PHI) are exempt from HIPAA. All other employer group health plans are subject to HIPAA. Health plans need to take immediate action to ensure that they meet the new HIPAA requirements.

New Breach Notice Requirements. Health plans have a new affirmative obligation to notify plan participants in the event of a breach of their unsecured PHI. This requirement will be enforced beginning **February 18, 2010.** "Unsecured PHI" is PHI that is not secured using a technology or methodology specified by the Secretary of Health and Human Services (HHS), for example encryption or destruction of material. Within 60 days of a breach, affected individuals must receive a notice with a description of what happened, when the breach occurred and when it was discovered. The notice must include the types of PHI involved, such as social security numbers, birth dates or diagnosis codes. Individuals must be informed of the steps they can take to protect themselves from potential harm. The health plan must provide contact information such as a web site, e-mail address or hot line number and take steps to mitigate a potential loss and prevent a reoccurrence. In the event the breach involves the PHI of more than 500 participants, notice must be given to a prominent media outlet and to the secretary of HHS for posting on its website. These breach provisions are in addition to any applicable state breach notification laws.

- Health plans need to revise their written HIPAA policies and procedures to address breach notifications and create breach response action plans.
- Health plans should re-examine their HIPAA Security policies and procedures, update business associate agreements, and re-check their compliance systems, especially with respect to vulnerable activities such as portable media (e.g., laptops, PDA and flash drives) and remote access to health information. Encryption of PHI using HHS approved applications can eliminate or minimize the risks of a breach of unsecured PHI and health plans should carefully consider encryption technologies as part of their HIPAA compliance

activities because using a technology or methodology specified by HHS, does not trigger the notification requirement.

Request for Restrictions on Certain Disclosures of PHI. When a health plan participant requests that the plan restrict the disclosure of PHI, the plan is obligated to comply with the request if it is for the purposes of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which the health care provider has been paid out-of-pocket and in-full. A plan no longer has discretion in complying with this request. Restriction request rules will be enforced as of **February 18, 2010.**

- Health plans must revise their HIPAA Notice of Privacy Practices, policies and procedures to reflect the new rights to request a restriction and inform participants of the change.

New Guidance on Minimum Necessary Standard. Health plans are required, except in cases of treatment and certain other purposes, to access, use and disclose only the *minimum necessary* amount of PHI needed to satisfy the purpose for which the data was acquired, used or disclosed. Under the new rules, health plans must first consider whether partially de-identified data, known as a limited data set, could be used to accomplish their objectives and must limit their uses and disclosures to limited data sets if possible. Under HITECH, HHS is required to establish guidance on what constitutes *minimum necessary* in the near future. The provision on using limited data sets to satisfy the minimum necessary standard goes into effect on **February 18, 2010** and remains in effect until the guidance is issued.

- Health plans will need to monitor HHS guidance on the minimum necessary standard and make changes in how they access, use and disclose PHI.

Accounting of Disclosures of PHI in Electronic Medical Records (EMR). Health plans must provide an accounting of disclosures of PHI made from the individual's medical record for the previous six years, upon request. Health plans using EMR will be required to include disclosures relating to treatment, payment and health care operations, although the accounting need only cover the previous three years. HHS is required to promulgate regulations to define what needs to be collected. Health plans may include disclosures from business associates in the accounting report they develop for plan participants and beneficiaries, or they can give individuals a list of the business associates involved in disclosing PHI from their records (and contact information) and direct them to request an accounting directly from the business associate. The business associate must comply with such a request. This will significantly increase administrative burdens for health plans, which currently are not required to account for such disclosures. This provision is subject to rulemaking and the earliest date it will apply is **January 1, 2011.**

- Health plans will need to monitor HHS guidance on the content of disclosures, consider the installation of software that tracks disclosures and revise their policies and procedures to update the scope of disclosure and compliance activities.

Direct Regulation of a Health Plan's Business Associates. A health plan's HIPAA compliance is only as good as that of the many business associates on which it relies for actuarial, claims processing, TPA, claims adjudication, legal, accounting, consulting, and other outsourced support functions and services. Among the most far reaching of the new changes are those that apply HIPAA's security rules and some of its privacy requirements directly to a health plan's business associates. Business associates will be directly regulated by HIPAA and subject to civil and criminal

penalties and enforcement proceedings for HIPAA violations. These new federal obligations for business associates are in addition to the contractual obligations that health plans have imposed on their business associates through business associate agreements. The direct regulation of business associates and their compliance with these HIPAA requirements will be effective as of **February 18, 2010.**

- Health plans need to audit their business associate relationships and ensure that they have business associate agreements in place.
- Health plans need to update their old business associate agreements to reflect the new HIPAA obligations and liabilities and set a very short time period for receiving a notice of breach, i.e., 5 business days and consider imposing "by-pass" accounting of disclosure obligations on business associates.
- As part of risk management and loss allocation strategies, health plans need to consider imposing performance standards on their business associates with respect to encryption, especially with respect to vulnerable activities such as portable media and remote access to health information. Health plans may also want to consider allocating the direct and indirect costs of notice to participants and mitigation costs to business associates in the business associate agreements, securing these obligations through insurance or performance bonds.

Penalties and Enforcement. Enforcement will be tougher and new penalties are dramatically higher, capping at $1.5 million per calendar year. The HIPAA enforcement team is expanded from US Attorneys General to include State Attorneys General. The HHS Office of Civil Rights is given audit rights and the authority to impose corrective action plans. Finally, individuals who are harmed by a violation of the privacy or security requirements of HIPAA will be eligible to receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such violation. HHS is directed to issue regulations by **February 17, 2012** that will establish the methodology. Aggressive enforcement of HIPAA is inevitable.

Butzel Long is prepared to assist clients with updating their group health plan language, notices of privacy practices, HIPAA privacy and security policies and procedures and business associate agreements, to comply with the changes to HIPAA under HITECH. We also are available to counsel clients on operational and technological compliance with HITECH.

If you would like more information about HIPAA compliance, please contact one of the authors of this E-News Alert, a member of the Employee Benefits Practice Group or your regular Butzel Long attorney.

Jordan Schreier
Phone: 734 213 3616
Email: schreier@butzel.com

Susan Patton
Phone: 734 213 3432
Email: patton@butzel.com

Butzel Long Employee Benefits Practice Group

Alexander B. Bragdon
Phone: 248 258 7856
Email: bragdon@butzel.com

Robert G. Buydens
Phone: 313 225 7013
Email: buydens@butzel.com

Roberta Granadier
Phone: 248 593 3020
Email: granadier@butzel.com

Mark W. Jane
Phone: 734 213 3434
Email: jane@butzel.com

Lynn McGuire
Phone: 734 213 3261
Email: mcguire@butzel.com

Antoinette M. Pilzner
Phone: 734 213 3630
Email: pilzner@butzel.com

Jordan Schreier
Phone: 734 213 3616
Email: schreier@butzel.com

Thomas L. Shaevsky
Phone: 248 258 7858
Email: shaevsky@butzel.com

Tara L. Slone
Phone: 734 213 3421
Email: slone@butzel.com

For previous e-news or to learn more about our law firm and its services,
please visit our website at: www.butzel.com

Butzel Long Offices:
Ann Arbor
Bloomfield Hills
Boca Raton
Detroit
Lansing
New York
Palm Beach
Washington D.C.

Alliance Offices:
Beijing
Shanghai
Mexico City
Monterrey

Member:
Lex Mundi