BUTZEL LONG
ATTORNEYS AND COUNSELORS

Automation Alley Newsletter

June 2009

HIPAA Hog Ties Business Associates: Enforcement Actions Rope Up Expensive Civil and Criminal Penalties

The American Recovery and Reinvestment Act of 2009 (commonly called the "Stimulus Law"), signed into law by President Obama on February 19, 2009 ushers in sweeping new changes in health information privacy laws in conjunction with providing billions of dollars in new federal stimulus funds to be spent on health information technology and electronic medical records. The Stimulus Law, which includes the Health Information Technology for Economic and Clinical Health Act, dramatically expands the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security standards by increasing the number of individuals and entities directly regulated by HIPAA. The Stimulus Law also significantly ramps up criminal and civil enforcement penalties for privacy breaches and creates a new private right of action for individuals to sue for privacy breaches. As it currently stands, compliance with these new requirements will be required by February 17, 2010. A brief overview of the most significant changes follows.

HIPAA Extends its Reach to Directly Regulate Business Associates

When patients seek help from health care providers and submit claims for payment to their health plans and insurers, they have the expectation that their personal health information will be kept private and that these providers and plans -- referred to as "covered entities" -- will use and disclose their private personal information on a strict "need to know" basis. To do their jobs, covered entities are permitted to use and disclose a patient's health information for the purpose of treatment, payment and operations without the individual's consent so long as they meet HIPAA's strict Privacy, Security and Administrative Rules. Covered entities are also able to share health information with their business associates who provide them with a wide array of functions including legal, billing, actuarial, marketing, strategic planning, fundraising, underwriting, customer services, accounting, data aggregation and management, consulting, collections, accreditation and other necessary support and outsourced services. As a result of the Stimulus Law, business associates are now subject to the HIPAA Security Rule in the same manner as it is applied to the covered entities for which they perform business functions. This means that business associates will face the same civil and criminal penalties for unauthorized use and disclosure of private information that HIPAA had originally only intended for covered entities. Business associate status is now expanded to apply to health information exchange organizations, regional health information organizations, e-prescribing gateways and vendors that contract with a covered entity to offer a personal health

record to patients as part of the covered entity's electronic health record. This effectively expands HIPAA regulations to anyone who services the health care industry and has access to health information.

The HIPAA Security Rule consists of a complex and comprehensive set of standards and implementation specifications that business associates must meet in order to comply with HIPAA by the February 17, 2010 effective date. The general requirements of the Security Rule require business associates to ensure the confidentiality, integrity and availability of all private health information that it creates, receives, maintains or transmits to and from covered entities. Business associates are required to put systems and technology in place to protect this information against reasonably anticipated threats or hazards to its security or integrity, including reasonably anticipated misuse or prohibited access by members of its workforce, subcontractors, agents, hackers and even thieves. To meet this broad mandate, the Security Rule is divided into five (5) major sections: all of which have either required or flexible implementation specifications.

1. Administrative safeguards are administrative actions, policies and procedures to select, develop, implement and maintain security measures to protect private information and manage the conduct of the business associate's work force, including the identification of a privacy officer.

2. Physical safeguards are physical measures, policies and procedures that protect systems, buildings and portable and fixed equipment from natural and environmental hazards and unauthorized intrusion, including hackers and theft.

3. Technical safeguards refer to the technology that protects private information and controls access to it through authentication and encryption, as well as audits its access and use.

4. Organizational requirements include the obligation of all downstream subcontractors and agents to also take steps to protect private information, including termination of subcontracts, if feasible, and if termination is not feasible, report to the Department of Health and Human Services (HHS).

5. Policies, procedures and documentation requirements require business associates to develop institutional standards, workforce training, human resources responses, technical responses and take other operational initiatives, such as corrective action plans and technology upgrades, to maintain compliance with the Security Rule.

Civil and Criminal Penalties for HIPAA Violations are Increased and Expanded

In the event of a HIPAA violation, covered entities and business associates will be subject to mandatory reporting requirements and must notify each affected individual. For breaches involving more than 500 affected individuals, there is mandatory media notification and Medicare notification. The new requirements will necessitate changes to business associate agreements and new forms. Civil money penalties in the event of a breach have increased dramatically from $100/ per violation (and an aggregate cap of $25,000) to:

1. $1,000 per violation for violations due to a reasonable cause and not willful neglect (and an aggregate cap of $100,000);

2. $10,000 per violation for violations due to willful neglect and is corrected (and an aggregate cap of $250,000); and

3. $50,000 per violation for violations due to willful neglect and is not corrected (and an aggregate cap of $1,500,000

The law now mandates certain enforcement measures, including requiring HHS to conduct periodic audits to ensure compliance. If HHS decides that a violation is due to willful neglect, the law requires that a penalty be imposed. In addition, state attorney generals can bring enforcement actions and obtain attorneys fees.

Harmed Patients Will Have a Right to Receive Distributions of Certain Civil Money Penalties Increasing Class Action Potential

Within the next three (3) years, HHS is required to issue regulations giving harmed patients a stake in any civil money penalty or monetary settlement collected with respect to certain HIPAA violations. When enacted, patients – and their attorneys – will have a powerful financial incentive to file complaints and to ensure that enforcement activities are pursued.

The above are just a few examples of the changes around the corner. There are other changes including those to the disclosure accounting provision and marketing restrictions. If you have any questions about the above, or would like our assistance in preparing for these changes, please contact your Butzel Long attorney, or any member of our Health Care Industry Team as indicated below.

Robert H. Schwartz	schwartzrh@butzel.com	248 258 2611
Susan H. Patton	patton@butzel.com	734 213 3432
Carol A. Romej	romej@butzel.com	734 302 1025
Julie A. Rajzer	rajzer@butzel.com	248 258 2610
Thomas L. Sparks	sparks@butzel.com	517 372 4372
Max R. Hoffman	hoffman@butzel.com	517 372 4374

Our team has also put together a comprehensive compliance checklist to help you assess your compliance needs. Please visit http://www.butzel.com/pdf/090521guiHCARE.pdf for a PDF version.

If you are interested in receiving future information regarding HIPAA or other Health Care related electronic bulletins, please visit http://www.butzel.com/pbsign.htm to sign up.