BUTZEL LONG
ATTORNEYS AND COUNSELORS

Automation Alley Newsletter

October 2009

HIPAA "MUST KNOW" "OR ELSE"

Important new personal health information privacy and security rules will have an enormous impact on the operations and use of technology by health care providers, health plans, health care clearinghouses and their business associates (who are now substantially, directly regulated in the same manner as covered entities). Health information privacy is a populist issue and critical to the trust required to take patient care and the health industry into the electronic age. Breaches of trust resulting from the unauthorized use and disclosure of **electronic protected health information (e-PHI)** will be subject to heightened enforcement efforts and stiff new penalties. Stringent new requirements will be paired with new, tiered, civil and criminal penalties, with all being serious and expensive, but especially egregious breaches resulting in fines of up to $1,500,000, mandatory disclosure to all individuals involved and mandatory notice to the media in the event that more than 500 individuals have PHI that is disclosed and which individuals may be damaged. Clients which possess health information have until mid-February 2010 to accomplish sea changes in the way they do business before the penalties apply, but compliance is expected as soon as mid-September, 2009.

The general requirements of HIPAA require that covered entities and business associates do the following:

1. Ensure the confidentiality, integrity, and availability of all the e-PHI the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.
4. Ensure compliance by the workforce.

Breach Notification Rules For Unsecured e-PHI

It is time to update policies and procedures, audit operations and IT to avoid strict new penalties. When the privacy of "unsecured" e-PHI is breached, new "breach notification rules" require health care providers, health plans, health care clearinghouses and their business associates to undertake an array of mandatory notifications, undertake mitigation strategies and indemnify for losses. An exception exists for "secured" encrypted information and for information that does not result in

a significant risk of financial, reputational or other harm to the individual as determined by a risk analysis in which the burden is on the covered entity or business associate to prove why breach notification is not required. The breach notification rules are the most recent of series of rules that HHS is issuing to implement new and stricter personal health information privacy and data security requirements for covered entities which were added to HIPAA under the **Health Information Technology for Economic and Clinical Health (HITECH) Act** signed into law on February 17, 2009 as part of American Recovery and Reinvestment Act of 2009 (ARRA/Stimulus Bill).

The new breach notification provisions require that covered entities and their business associates undertake the following mandatory actions:

- Notice to patients of breaches within 60 days, from the date the breach was actually discovered or the date it should have been discovered by exercising reasonable diligence
- Notice to covered entities by business associates when business associates discover a breach of their own or that of a subcontractor or agent
- Notice to "prominent media outlets" on breaches of 500 individuals or more
- Notice to "next of kin" on breaches of patients who are deceased
- Notice to the Secretary of HHS of breaches of 500 or more
- Annual notice to the Secretary of HHS of breaches of less than 500 of "unsecured PHI" that pose a significant financial risk or other harm to the individual, such as financial or reputation harm.

The new rules also establish mitigation minimums and indemnification minimums. Mitigation minimums include toll free numbers, web sites, credit reporting and counseling, among other expensive actions.

Exceptions to the breach notification requirements, include inadvertent "peeks" and "disclosures" of e-PHI by otherwise authorized individuals in situations where the information is not disclosed further and breaches involving e-PHI secured through encryption.

Encryption Rules to Create Secure e-PHI

New encryption rules published on April 17, 2009 establish exactly when and how e-PHI is "secured" in its various data states: 'data in motion' (i.e., data that is moving through a network, including wireless transmission); 'data at rest' (i.e., data that resides in databases, file systems, and other structured storage methods); 'data in use' (i.e., data in the process of being created, retrieved, updated, or deleted); or 'data disposed' (e.g., discarded paper records or recycled electronic media).' While styled as "guidance," the encryption rules are very directive. Covered entities and their business associates should encrypt data in all data states in accordance with HHS standards found in NIST 800-111 and FIPS 140-2. Individuals and organizations that meet these encryption requirements have suitably "secured" their e-PHI and rendered it "unusable, unreadable or indecipherable to unauthorized individuals." Breaches of "secured" e-PHI are exempt from the onerous breach notification rules described above.

FTC Rules for Internet Based Businesses

On August 17, 2009, the FTC issued rules that require some Internet based businesses to notify consumers when the business has experienced a breach of unsecured e-PHI. The FTC notification requirements are similar to those required by HIPAA.

Enforcement Dates and Summary

These new HIPAA rules will have a practical impact on all aspects of business operations, including the use of portable work stations, laptops, blackberries and other hand held devices, storage, transmission standards, technology upgrades business processes, encryption, passwords, physical floor plan layouts, storage and destruction of electronic protected health information e-PHI, insurance and risk management, personnel training and disciplinary actions against personnel involved in breaches of e-PHI.

The Secretary of HHS has announced a moratorium on enforcement actions for an additional period of time to give covered entities and their business associates time to comply with the new rules. In response to claims that the Center for Medicare and Medicaid Services (CMS) was dodging its enforcement responsibilities, HIPAA enforcement has been transferred to the Office of Civil Rights (OCR). By mid-February 2010, expect an actions to begin in earnest.

How Butzel Can Help

- Advise business associates on how to comply with privacy and security rules
- Update business associate agreements to address the new security and notification requirements
- Draft breach notification policies and procedures
- Review and revise privacy policies and procedures, including human resources policies and procedures
- Conduct workforce training sessions and advise Privacy Officers
- Facilitate security audits and gap analyses
- Conduct risk management and insurance reviews
- Update Notice of Privacy Practices

Members of Butzel Long's HIPAA Task Force are ready to assist covered entities and business associates meet these challenges and take necessary steps to protect themselves. For more information, please contact any member of the HIPAA Task Force.

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
Debra A. Geroux	geroux@butzel.com	517 372 4373
Christopher M. Taylor	taylorc@butzel.com	734 213 3605
Alan Lambert, M.D.	lambert@butzel.com	212 905 1513
Omar N. Chaudhary	chaudhary@butzel.com	734 213 3437

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.

The above news is only intended to highlight some of the important issues. This e-mail has been prepared by Butzel Long for information only and is not legal advice. This information is not intended to create, and receipt of it does not constitute, a client-lawyer relationship. Readers should not act upon this information without seeking professional counsel. This electronic newsletter and the information it contains may be considered attorney advertising in some states. If you feel you have received this information in error, or no longer wish to receive this service, please follow the instructions at the bottom of this message.

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