BUTZEL LONG

Client Alert:
Health Care

www.butzel.com

February 14, 2013

HIPAA Mega Rule Action Plan

The HIPAA Mega Rule published on January 25, 2013 reinforces the government's commitment to protecting the privacy of protected health information (PHI) and also aggressively pushes electronic health records and office practices into the electronic age through a system of financial incentives and penalties. The Mega Rule provides the public with increased protection and control over PHI. The Mega Rule has operational, financial and legal implications that will affect all providers.

ACTION STEPS
Providers should take steps to:

- Revise Notice of Privacy Practices
- Inventory all relationships between providers and contractors
- Make Business Associate Agreements HITECH-Compliant
- Evaluate Subcontractors for Business Associate Status
- Make regulated Subcontractors HITECH-Compliant
- Revise breach risk assessment
- Revise HIPAA Policies and Procedures
- Anticipate a breach or audit, and create an incident response plan

Time is of the essence as there are short compliance deadlines for implementing changes mandated by the Mega Rule. The expanded enforcement powers of the Office for Civil Rights are effective on **March 26, 2013**. Notices of Privacy Practices must be updated and posted on or promptly after the effective date of **March 26, 2013**. The compliance deadline is September 23, 2013 for new Business Associate Agreements and not later than **September 23, 2014** for existing Business Associate Agreements, unless they expire or will be renewed prior to **September 23, 2014**.

A lot of work will need to be done to meet these deadlines. Pressure will be added by the robust HIPAA random audits now funded, staffed and underway, which are in addition to "for cause" audits in response to a complaint or a breach.

Expanded Definition and Liability of Business Associates Includes Subcontractors: The Mega Rule's expanded definition of Business Associates now includes subcontractors of Business Associates who create, receive, maintain or transmit PHI, regardless of how many levels of subcontracting or outsourcing occur, and even if PHI is never accessed. Many common relationships that did not previously involve a Business Associate Agreement will now require HITECH-Compliant Business Associate Agreements.

HITECH-Compliant Business Associate Agreements: The Mega Rule mandates new content in the Business Associate Agreement to comply with HITECH. Mandatory new provisions include those requiring Business Associates to enter into written HITECH-Compliant Business Associate Agreements with their subcontractors, regardless of tier.

The scope of services in the "prime" Business Associate Agreement between the provider, as covered entity, and the first-tier downstream Business Associates will control much of the content in these subcontractor agreements, in addition to requirements of HITECH and the Mega Rule.

FINES AND PENALTIES: The Mega Rule increases the fines and penalties for data breaches and assesses them "per violation" up to the maximum penalty of $1.5 million. As a result, the fines and penalties arising out of data breaches are significant and can add up fast. Business Associates and their subcontractors are now directly liable for the same regulatory penalties and sanctions as providers, as covered entities, have been. All providers and their downstream contractors must address their legal risks and compliance strategies in the Agreements. These are not mandated by the Mega Rule but are necessitated by liability, risk management and allocation of risk of loss concerns. Insurance and indemnification issues should require a great detail of attention in the new Business Associate Agreements.

Revised Breach Notification Rule: As a result of changes in the breach notification rule, more providers will be required to provide notice of breaches. In the event of a breach of unsecured, non-de-identified PHI, the former "risk of harm" assessment becomes the "assessment of probability that PHI has been compromised" taking into account at least the following factors: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii)whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated. If an evaluation of the factors discussed above fails to demonstrate that there is a low probability that PHI has been compromised, breach notification is required. Breach notification may be to the persons affected, to the Secretary of Health and Human Services, or to the media. Breach notifications and remediation is expensive, time consuming and costly in terms of reputation and public trust.

Patient Rights Expanded: The Mega Rule expands the right of individual patients to control their PHI in several important ways that will create operational headaches for providers. Currently, individuals have the right to request restrictions to the use and disclosure of their PHI, but providers may decline to agree to them. Under the Mega Rule, if a patient pays for service "in full," the provider is required to comply with the request. Patients are entitled to receive to their PHI in an electronic form if the provider maintains PHI electronically and if the PHI is readily producible in the requested form. The Mega Rule also strengthens privacy protections for certain genetic information under the Genetic Information Nondiscrimination Act ("GINA"). Providers and their Business Associates have new limits placed on their uses and disclosures of PHI in marketing and fundraising. Patients have the right to opt out or marketing and fundraising contacts. Financial remuneration is regulated. Providers cannot sell PHI without an individual's authorization except in very limited circumstances.

Notice of Privacy Practices Updated to Incorporate Expansion of Patient Rights: Providers are required to update their Notice of Privacy Practices to disclose the expanded patient rights. New patients must sign an acknowledgement of receipt of the Notice of Privacy Practices, but current patients only need to see a copy of a posted Notice and have an opportunity to obtain a personal copy for themselves without having to ask a receptionist.

HIPAA Enforcement Authority Strengthened in Enforcement Rule: Providers must expect more investigations and audits. The Office for Civil Rights has been given new muscle to investigate complaints of breaches of PHI, including investigations of complaints suggesting willful neglect of privacy or security standards. Investigations remain discretionary for complaints suggesting non-willful neglect, but the Office for Civil Rights has commented that it will proceed with

an investigation in every situation where the facts indicate a possible violation of HIPAA. Providers may correct non-compliance by voluntary corrective action, but there may be circumstances where direct formal enforcement is undertaken by OCR. HITECH imposed for tiers of "badness" which increase penalty amounts that correspond with escalating tiers of culpability.

Significantly, providers are made liable for the acts and omissions of their Business Associates who are agents of the provider in accordance with the federal common law of agency. This liability is also directly applied to Business Associates and members of its workforce acting within the federal common law of agency. However, the fact that a provider has a HITECH-Compliant Business Associate Agreement with a contractor is not dispositive. Finally, the Mega Rule promulgated five general factors that the Office for Civil Rights will weigh in determining the amount of a civil money penalty for a HIPAA violation.

Implementation of Mega Rule Action Plan: Members of the Butzel Long Health Care Law Group are ready to help providers implement their HIPAA Mega Rule Action Plans. We encourage clients and other providers affected by this rule to work diligently to meet the compliance deadlines and ready their organizations and members of their workforce to respond to inevitable HIPAA challenges including patient complaints and requests, privacy and security breaches, and to prepare for Office for Civil Rights audits.

If you have any questions about this Client Alert, please contact your regular Butzel Long attorney, a member of the Butzel Long Health Care Industry Group, or the author of this alert.

Susan H. Patton
734.213.3432
patton@butzel.com

Health Care Industry Group

Debra A. Geroux
248.258.2603
geroux@butzel.com

Adele P. Jorissen
248.258.7864
jorissena@butzel.com

Mark R. Lezotte
313.225.7052
lezotte@butzel.com

Thomas R. McAskin
248.258.2511
mcaskin@butzel.com

Susan H. Patton
734.213.3432
patton@butzel.com

Robert H. Schwartz
248.258.2611
schwartzrh@butzel.com

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.

Attorney Advertising Notice - The contents of this e-mail may contain attorney advertising under the laws of various states. Prior results do not guarantee a similar outcome.

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
Detroit
Lansing
New York
Washington D.C.

Alliance Offices:
Beijing
Shanghai
Mexico City
Monterrey

Member:
Lex Mundi