

August 2009

## HIPAA Alert

### New HIPAA Breach Notification Regulations Require Immediate Attention

On August 19, 2009, the U.S. Department of Health and Human Services (“HHS”) posted an “advance copy” of its final HIPAA breach notification regulations on the HHS website. These regulations are expected to be published in the Federal Register on August 24, 2009. Once published, covered entities and business associates will, as a practical matter, **only have 30 days to comply with the new rules—a very short time** and one which will force them to work very diligently to comply with the new rules.

Background. The American Recovery and Reinvestment Act (“the Act”) from February 2009 (also known as the Stimulus Bill) contained a section called the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”). The main purpose of the HITECH Act was to further promote electronic communication in the health care area. For example, the HITECH Act promotes the use of “electronic health records” of individuals, in an effort to move away from a paper-based health care system.

The HITECH Act also made changes to the HIPAA Privacy and Security Rules. These changes have varying effective dates, including the following:

- Increased penalties—generally effective February 2009
- New breach notification rules—generally effective 30 days after publication of the rules in the Federal Register (here, the expected deadline is September 23, 2009)
- New restriction request rules—generally effective February 2010
- New prohibitions on sale of protected health information (“PHI”)—generally effective February 2011
- Certain rules relating to electronic health records—generally effective January 2011 (can be later)

We described each of these changes in more detail in our prior client alert titled, “Stimulus Bill Dramatically Modifies HIPAA Rules—Business Associates and Covered Entities Must Address New Requirements.” This alert focuses only on the new breach notification rules.

Effective Date of New Breach Notification Rules. If there is a “breach” of PHI (including oral, written or electronic PHI), the breach must be reported to HHS and, as discussed below, may need to be reported to an affected individual and to the media. **For calendar year 2009, covered entities and business associates must report to HHS and the affected individuals all breaches which occur 30 days after the regulations are published—approximately September 23, 2009.** HHS will use its “enforcement discretion” and not impose



any HHS-related penalties for the first 180 days after publication of the regulations (approximately February 23, 2010). Unfortunately, this enforcement discretion does not mean a covered entity or business associate need not comply with the new rules until February 23, 2010. A covered entity and business associate must be able to identify, record, investigate, and report to an affected individual and HHS any breach occurring after September 23, 2009. **This will require covered entities and business associates to update all their business associate agreements, train their workforces and establish their policies and procedures to ensure that they can identify, record and report such breaches.** This will be a lot of work for covered entities, but even more work for business associates. Business associates previously did not need to have any HIPAA policies and procedures but now must immediately create such policies and procedures, train their workforces, and track and report breaches.

Complying by the effective date may be difficult for many entities. For example, many multiemployer plans or governmental entities have boards with authority to adopt the new policies required under the regulations. However, these boards may meet only quarterly. The boards may need to have a special meeting prior to the next regularly-scheduled meeting to adopt new policies and procedures by September 23, 2009.

Michael Best to Provide Assistance. We have already updated our Business Associate and Group Health Plan HIPAA Privacy and Security Compliance Forms for the HITECH Act. In the next few days, we will update the Compliance Forms for these new regulations. Licensees who obtain the Compliance Forms will also receive a new feature—a **free 90-minute pre-recorded training video** on the Compliance Forms and the HIPAA Privacy and Security Rules. This video will assist in training the workforce of a covered entity or business associate. The updated Compliance Forms are expected to be available by August 28, 2009. Prices for the Compliance Forms are as follows:

- Group Health Plan HIPAA Privacy Compliance Forms
  - Regular License \$400
  - Expanded License \$1,200
- Group Health Plan HIPAA Security Compliance Forms
  - Regular License \$400
  - Expanded License \$1,200
- Business Associate HIPAA Privacy Compliance Forms \$400
- Business Associate HIPAA Security Compliance Forms \$400

Discounts: If you order two Regular Licenses, a \$100 discount applies (e.g., you can obtain the Group Health Plan HIPAA Privacy and Security Compliance Forms for \$700 instead of the typical \$800 cost). If you order two Expanded Licenses a \$400 discount applies (e.g., you can obtain the Group Health Plan HIPAA Privacy and Security Compliance Forms for \$2,000 instead of the typical \$2,400 cost). If you are a prior licensee of the Compliance Forms we will provide an additional \$100 discount.

The “Regular License” generally allows a covered entity to use the materials for its own compliance purposes and to distribute materials (e.g., a business associate agreement) as needed. Some entities, such as third-party administrators, benefit consultants and insurance brokers, wish to provide the materials to all their clients. The “Expanded License” generally allows such use.

To receive more information visit our web site at [michaelbest.com/HIPAA](http://michaelbest.com/HIPAA) or check the appropriate boxes above and fax this page to Linda Woyach at Michael Best, fax number 414.277.0656, along with your contact information. We will then send you additional information.

“Breach” Definition Modified. The regulations provide that a “breach” exists if there is an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rules and such action “compromises” the security or privacy of the PHI. HHS expanded upon the definition of “compromises” to include a helpful “risk” analysis. PHI is “compromised” only if the event poses a “significant risk of financial, reputational, or other harm to the individual.” Presumably many minor, insignificant breaches will not pose a significant risk of financial, reputational or other harm. Such breaches generally need not be reported to the affected individual or to HHS.

An additional, helpful change was made to the definition of “breach”. If there is an inadvertent disclosure of PHI by a person who is not authorized to access PHI, the disclosure will not be a “breach” if the PHI is not further used or disclosed in a manner that violates the Privacy Rules.

Notification to Individuals. The text of the regulations provides that a covered entity—not a business associate—is responsible for notifying individuals of a PHI breach. (Presumably a business associate could, by contract, agree to provide such notice.) Covered entities and business associates must negotiate how quickly the business associate will notify the covered entity of the breach. Business associates likely will also need to negotiate with their third-party service providers who receive PHI (an agent/subcontractor) to ensure that such service providers notify the business associate of any breach.

Practical Tip: All covered entities and business associates should set out to immediately identify all their business associates (or, for business associates, their agents/subcontractors) and modify the relevant agreements to include these new regulations. The Michael Best Compliance Forms include a business associate agreement reflecting these new changes.

The covered entity must notify affected individuals without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. HHS emphasizes that 60 days is an outer limit and that, in some situations, 60 days would be unreasonable.

Insufficient Contact Information. The regulations specify what notice must be provided if there is insufficient contact information for a group of individuals affected by a breach. If insufficient information is available for more than 10 individuals, a covered entity must use an “alternative form” to contact the individual. The alternative form must be either a posting on the web site of the covered entity or “conspicuous notice” in major print or broadcast media.

Practical Tip: Many group health plans may not currently have their own web site. However, many group health plans likely would be reluctant to notify major print or broadcast media of a breach. Thus, many group health plans should consider creating a web site, perhaps solely for the purpose of posting breach notices where there is insufficient contact information.



Notification to Next of Kin. If the individual affected by the breach has died, the covered entity must notify the individual's next of kin or personal representative of the breach, if the covered entity has contact information for the next of kin or personal representative.

Major Breach—Notification to Media. If a breach affects 500 or more individuals, the covered entity (not the business associate) must notify "prominent media outlets" in the relevant state or jurisdiction. HHS notes that it received requests to define what media outlets would be considered "prominent." However, it declined to do so, essentially noting that this is a facts and circumstances test.

Major Breach—Notification to HHS. The regulations retain the rule under the HITECH Act that a major breach of 500 or more individuals must be reported to HHS. The HITECH Act required that such notice be "immediate". The word "immediate" caused concern that notice could be required in a very short time period, perhaps only a few days (or less). The regulations are helpful and provide that notice to HHS must be sent at the same time the affected individual is notified. This standard is also more lenient than the Federal Trade Commission's ("FTC") standards interpreting the HITECH Act, which requires notice to the FTC within 10 business days. (The FTC rules are not applicable to most covered entities or business associates.)

When a Breach is "Discovered". A breach will be "discovered" on the date that it is known or, if the business associate or covered entity exercised "reasonable diligence", would have been known. HHS clarifies that "reasonable diligence" means the "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances." HHS also clarifies that a business associate or covered entity will generally "know" everything that its agents "know". For example, if a business associate's agent or subcontractor knows of a PHI breach, the business associate will be deemed to know about the breach. The regulations specify that an "agent" will be determined in accordance with the federal common law of agency. The federal common law of agency is not always clearly defined (see, e.g., Joshua A. T. Fairfield, "ERISA Preemption and the Case for a Federal Common Law of Agency Governing Employer-Administrators," 68 U. Chi. L. Rev. 223 (2001)).

Practical Tip: Business associates and covered entities will need to carefully identify their "agents" and ensure that they have an appropriate agreement in place with these agents. The agreement should specify that the agents will notify the business associates and covered entities of any PHI breaches and should also specify the information to be reported and the time period in which to report.

Law Enforcement Delay. The regulations provide an exception to the notification rules if a delay is requested by law enforcement. If the law enforcement request is in writing, the delay must last for the requested time period. If the request is made orally, the covered entity or business associate must document the identity of the official making the statement and accommodate the request, but for no longer than 30 days.



Training. The regulations explicitly provide that a covered entity's workforce must be trained on the new breach notification regulations. It appears that a business associate's workforce also must be trained on the new regulations, although this is not completely certain.

Practical Tip/Roadmap: Before training can be accomplished, revised policies and procedures must be created. Thus, covered entities and business associates should: (1) review the new changes under the regulations; (2) identify all business associates and agents/subcontractors; (3) update all agreements with such business associates and agents/subcontractors to include the new requirements; (4) prepare the new forms and policies and procedures required by the regulations; (5) train the relevant workforces; and (6) prepare for contingencies (e.g., create a website for a covered entity, if none exists, in order to post breach notification information).

Complaints. The regulations explicitly provide that a covered entity must provide a process for individuals to complain about the covered entity's policies and procedures relating to the breach notification process. (The right to complain existed in the original HIPAA regulations and in general is not a change.)

Practical Tip: Many covered entities describe the right to complain in a notice of privacy practices. A covered entity should review its notice of privacy practices to determine whether it must be updated to specifically include the right to complain about the breach notification process. If the notice must be updated, the covered entity will then need to re-distribute the notice to appropriate individuals.

Sanctions. The regulations explicitly provide that a covered entity (and perhaps a business associate) must include in its policies sanctions for violating the new breach notification rules.

Practical Tip: A covered entity or employer should examine its handbook or other provisions regarding sanctions to ensure that they are broad enough to include sanctions relating to the new breach notification rules. If not, the handbook or other provisions must be updated.

For more information contact, please contact John L. Barlament at 414.225.2793, or [JLBarlament@michaelbest.com](mailto:JLBarlament@michaelbest.com), your regular Michael Best & Friedrich LLP attorney or one of the following: Charles P. Stevens at 414.225.8268, or [CPStevens@michaelbest.com](mailto:CPStevens@michaelbest.com); Kirk A. Pelikan at 414.223.2529, or [KAPelikan@michaelbest.com](mailto:KAPelikan@michaelbest.com); Sarah L. Fowles at 414.225.4982, or [SLFowles@michaelbest.com](mailto:SLFowles@michaelbest.com); Kate L. Bechen at 414.225.4956, or [KLBechen@michaelbest.com](mailto:KLBechen@michaelbest.com).

In accordance with applicable rules, this material may be considered advertising.

This Alert is a publication of Michael Best & Friedrich LLP and is intended to provide clients and friends with information on recent legal developments. This Alert should not be construed as legal advice or an opinion on specific situations. For further information, feel free to contact article authors or other members of the firm. We welcome your comments and suggestions regarding this publication. © 2009 Michael Best & Friedrich LLP. All rights reserved.

