BALCH & BINGHAM LLP
Alabama • Georgia • Mississippi • Washington, D.C.

HEALTHCARE BULLETIN

August 31, 2009

INCREASED ADMINISTRATIVE BURDENS ACCOMPANY HHS BREACH NOTIFICATION REQUIREMENTS

On August 24, 2009, the Department of Health and Human Services ("HHS") issued new regulations requiring health care providers, health plans, and other entities subject to the Health Insurance Portability and Accountability Act ("HIPAA") to notify individuals and potentially HHS when their unsecured protected health information is breached. The regulations implement breach notification requirements enacted under the Health Information Technology for Economic and Clinical Health ("HITECH") Act, part of the American Recovery and Reinvestment Act of 2009 ("ARRA").

Background

The HITECH Act requires HIPAA covered entities to promptly notify affected individuals of a breach of unsecured protected health information ("PHI"), as well as the HHS Secretary and the media when a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals must be reported to the HHS Secretary on an annual basis. The HITECH Act also requires business associates of covered entities to notify the covered entity of breaches at or by the business associate.

The HITECH Act defines "unsecured" PHI to mean PHI that is not secured through the use of a technology or methodology required in HHS guidance to render PHI "unusable, unreadable, or indecipherable to unauthorized individuals." After consulting with information security experts, HHS issued guidance on April 17, 2009 identifying two methods for securing and rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction. If a covered entity chooses to encrypt PHI to comply with the Security Rule, does so pursuant to the HHS guidance, and subsequently discovers a breach of that encrypted information, the covered entity will not be required to provide breach notification because the information is not considered to be unsecured PHI.

Interim Final Rule

As explained in more detail below, the interim final rule largely follows the HITECH Act requirements with several important clarifications and modifications.

A. Obligations of Covered Entities

The interim final rule requires covered entities to notify each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed following a breach of that unsecured PHI. The interim final rule sets forth the following three step process for determining when a breach notification must be made:

Step One: The covered entity must determine whether there has been an impermissible use or disclosure of unsecured PHI under the HIPAA Privacy Rule.

Step Two: Once it is established that a use or disclosure violates the HIPAA Privacy Rule, the covered entity must determine whether the violation compromises the security or privacy of the unsecured PHI. A breach will be deemed to have compromised the security or privacy of unsecured PHI if the use or disclosure "poses a significant risk of financial, reputational or other harm to the individual." Thus, to determine if an impermissible use or disclosure of unsecured PHI constitutes a breach, covered entities must perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure.

In some cases, the unsecured PHI may be recovered so quickly (such as with the recovery of a lost laptop computer when forensic analysis shows that no PHI has been opened, altered, transferred or otherwise compromised) or is so limited in content, that the risk of harm is low enough that a breach notification may be avoided. Caution is advised when conducting such analyses, however, as the interim final rule places the burden of demonstrating compliance squarely on the shoulders of the covered entity.

Step Three: Finally, a covered entity must determine whether the incident is excluded from the definition of "breach" because it is: (i) an unintentional use of unsecured PHI by a workforce member acting in good faith and within the scope of his or her authority, and the unsecured PHI is not further used or disclosed improperly; (ii) an inadvertent disclosure of unsecured PHI by an authorized person to another authorized person, and the unsecured PHI is not further used or disclosed improperly; or (iii) a disclosure of unsecured PHI to an unauthorized person where there is a good faith belief that the unauthorized person would not reasonably have been able to retain the unsecured PHI.

If information is de-identified in accordance with 45 C.F.R. 164.514(b), it is not protected health information, and thus, any inadvertent or unauthorized use or disclosure of such information will not be considered a breach. The interim final rule also establishes a narrow exception for a use or disclosure of unsecured PHI that

excludes the sixteen direct identifiers listed at 45 C.F.R. 165.514(e)(2) as well as dates of birth and zip codes.[1]

B. Content of Notification

Notifications must be written in plain language and must include, among other things: (i) a brief description of what happened, including the date of the breach and the date of discovery of the breach, if known; (ii) a description of the types of unsecured PHI subject to the breach; (iii) steps individuals should take to protect themselves from potential harm resulting from the breach; (iv) a brief description of the steps the covered entity is taking to investigate the breach, mitigate harm, and protect against future breaches; and (v) contact information for individuals to ask questions or obtain additional information, including a toll-free number, email address, website, or postal address.

C. Methods of Notification

Notices must be delivered by first-class mail to the last known address of the affected individual or via email if the affected individual has agreed to email and has not withdrawn such agreement. If a covered entity does not have sufficient contact information for some or all of the affected individuals, or if some notices are returned as undeliverable, the covered entity must provide substitute notice for the unreachable individuals. If there are fewer than ten individuals for whom the covered entity has insufficient or out-of-date contact information, the covered entity must provide substitute notice through an alternative form of written notice, by telephone or other means (e.g., a conspicuous posting on the home page of the covered entity's website). If the contact information for ten or more individuals is found to be outdated or insufficient, the covered entity must provide substitute notice in one of the following forms:

(1) Conspicuous posting on the home page of the covered entity's website for a period of no fewer than 90 days; or

(2) In newspaper or broadcast media, including the geographic areas where the individuals affected by the breach likely reside.

In addition, the substitute notice on the website or in print or broadcast media must include a toll-free telephone number that will remain active for 90 days where individuals can learn whether their unsecured PHI was included in the breach.

[1] The sixteen direct identifiers include: (i) names; (ii) postal address information, other than town or city, state, and zip codes; (iii) telephone numbers; (iv) fax numbers; (v) email addresses; (vi) social security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) web Universal Resource Locators (URLs); (xiv) internet Protocol (IP) address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full face photographic images and any comparable images.

D. Timing of Notice

Covered entities must deliver notices to individuals "without unreasonable delay" but no later than 60 calendar days after discovery of the breach. Breaches will be treated as "discovered" on the first day that the breach is known to the covered entity, or when, by exercising reasonable diligence, the breach would have been known to the covered entity. As HHS expects covered entities to make the individual notifications as soon as reasonably possible, covered entities may not delay in commencing investigations or in sending the required notices. However, covered entities are expected to take a reasonable time to collect the information required for the notice. Consequently, in some cases multiple mailings may be needed as information becomes available.

The requirement that no "unreasonable delay" occur prior to notification highlights the importance of appropriately training employees, managers and other agents to notify the Privacy Official immediately when a potential breach occurs.

E. Notice to HHS and the Media

Covered entities are also required to notify the HHS Secretary upon the occurrence of a breach. For breaches involving the unsecured PHI of more than 500 individuals, Covered Entities must "immediately" notify the HHS Secretary. HHS has interpreted the term "immediately" to mean within the same time frame established for notifying affected individuals. In addition, if the breach involves the unsecured PHI of more than 500 individuals who reside in the same state or jurisdiction (e.g., city or county), the covered entity must notify "prominent local media outlets" of the breach. There is no uniform definition of a "prominent local media outlet." Depending on circumstances, an appropriate media outlet may include a local television station or a major general interest newspaper with a daily circulation throughout an entire state.

For breaches involving the unsecured PHI of fewer than 500 individuals, covered entities must maintain a log or other documentation of the breach and submit information annually to the HHS Secretary for breaches occurring during the preceding calendar year. The annual notices must be provided within 60 days of the end of each calendar year.

F. Obligations of Business Associates of Covered Entities

The interim final rule requires a business associate of a covered entity to notify the covered entity when it discovers a breach of unsecured PHI. A breach will be treated as "discovered" by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. The business associate must provide notice of a breach to a covered entity without unreasonable delay, but in no case later than 60 days following the discovery of a breach. To the extent possible, business associates must provide affected covered entities with the identity of each individual whose unsecured PHI has been, or is reasonably believed to have been, breached.

If a business associate is acting as an agent of a covered entity, then the business associate's discovery of the breach will be imputed to the covered entity. Accordingly, in such circumstances, the covered entity must provide notification to affected individuals and the HHS Secretary based on the time the business associate discovers the breach. If the business associate is acting as an independent contractor, then the covered entity must provide notification based on the time the business associate notifies the covered entity of the breach.

G. Effective Date

The interim final rule will apply to breaches of unsecured PHI that occur on or after 30 days from publication of the rule in the Federal Register. The interim final rule was published in the Federal Register on August 24, 2009, and will therefore become effective on September 23, 2009. HHS has indicated that it will use its enforcement discretion to not impose sanctions for failure to provide the required notifications for breaches that are discovered within 180 calendar days from the publication of the interim final rule in the Federal Register. However, covered entities and business associates are expected to comply with the breach notification regulations during this interim period.

As noted above, the rule applies to breaches that are discovered 30 or more days after the interim final rule's publication in the Federal Register. HIPAA covered entities and business associates must act quickly to implement the requirements set forth in the interim final rule. Steps to take include the following:

(1) Determine whether protected health information is "secured" in accordance with the Privacy Rule and HHS guidance. If an organization's PHI is not secured, the organization should make a determination whether to implement the technologies that will render the PHI unusable, unreadable, or indecipherable to unauthorized individuals in accordance with the HHS guidance.

(2) Develop policies and procedures for breach notifications and securing PHI, including guidelines for determining whether a breach that requires notice has occurred.

(3) Revise business associate agreements to address breach notice obligations.

(4) Train workforce members (e.g., employees, officers and agents) regarding the new breach notice requirements.

***

Should you have any questions, please do not hesitate to contact one of our healthcare attorneys at the offices below.

HEALTHCARE CONTACTS

BIRMINGHAM, AL

Matthew A. Aiken
205.226.3425
maiken@balch.com

Colin H. Luke
205.226.8729
cluke@balch.com

Jack B. Levy
205.226.8750
jlevy@balch.com

MONTGOMERY, AL

Dorman Walker
334.269.3138
dwalker@balch.com

ATLANTA, GA

Richard D. Sanders
404.261.6020
rsanders@balch.com

Philip M. Sprinkle, II
404.261.6020
psprinkle@balch.com

GULFPORT, MS

H. Rodger Wilder
228.214.0412
rwilder@balch.com

JACKSON, MS

Dinetia Newman
601.965.8169
dnewman@balch.com