



Employee Benefits Law Information Memo

September 2009

Electronic Dispatch

[Go to BS&K Employee Benefits Law Home Page](#)

HIPAA SECURITY BREACH NOTIFICATION RULES REQUIRE IMMEDIATE ACTION BY COVERED ENTITIES AND BUSINESS ASSOCIATES

Among other things, the Health Insurance Portability and Accountability Act ("HIPAA") requires health care plans, third party health plan administrators, pharmacy benefit managers, health care providers, and other so-called "covered entities" and "business associates" to maintain the confidentiality and security of an individual's "protected health information" or "PHI." The Health Information Technology for Economic and Clinical Health Act ("Act"), enacted earlier this year as part of the economic stimulus package, introduced substantial changes to the HIPAA privacy and security rules, including the addition of new notification requirements that may apply in the event that the privacy or security of PHI is compromised.

Under the Act, if the confidentiality or security of PHI is compromised by a "covered entity," notification of the "breach" may have to be provided to (i) affected individuals, (ii) the United States Department of Health and Human Services ("HHS"), and (iii) in certain cases, the media. If a "business associate" compromises the confidentiality or security of PHI, the business associate may be required to notify the covered entity of the breach.

On August 24, 2009, HHS issued interim final rules ("Final Rules") that clarify the breach notification requirements. Although the Final Rules are effective September 23, 2009, and although HHS expects covered entities to comply as of that date, sanctions will not be imposed for noncompliance that occurs prior to February 23, 2010. Until then, HHS has indicated that it will take appropriate corrective action to help covered entities achieve compliance. Covered entities and business associates should not delay implementing appropriate measures to comply with the requirements of the Final Rules, despite the delayed enforcement date.

Covered Entities, Business Associates and PHI Defined

For purposes of the Final Rules, a "covered entity" is defined as a health plan, health plan clearinghouse, or health care provider that transmits any health information electronically in connection with a covered transaction (such as submitting health care claims to a health plan). A "business associate" is defined as a person who performs functions on behalf of, or certain services for, a covered entity that involve the use or disclosure of individually identifiable health information (e.g., third party administrators or pharmacy benefit managers for health plans). PHI is defined as individually identifiable health information held or transmitted by HIPAA covered entities and business associates, subject to certain limited exceptions.

When Does a Breach Occur?

The Final Rules define a breach to mean the unauthorized acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of such information. The security or privacy of PHI is considered to be "compromised" under the Final Rules if its disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

HHS previously issued guidance regarding when PHI is considered "secure," and therefore not subject to the breach notification requirements. Generally, the guidance stated PHI is not considered secure unless it is either destroyed or encrypted in accordance with National Institute of Standards and Technology guidelines.

Under the Final Rules, a breach does not include certain unintended and inadvertent disclosures of unsecured PHI, nor disclosures where the recipient would not have been able to retain the disclosed information (e.g., instances where unsecured PHI is mailed to the wrong individual and the envelope is returned unopened).



What are the Notification Requirements With Respect to Individuals?

General Requirement: After the discovery of a breach of unsecured PHI, the Final Rules require covered entities to notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach. Breaches are treated as discovered as of the first day that the covered entity knows, or reasonably should have known, of the breach.

Timing of Notice: The notification must be provided without “unreasonable delay” (i.e., as soon as reasonably possible) and in no event later than 60 calendar days after the breach is first discovered by the covered entity.

Content of Notice: The notification must include, to the extent possible: (1) a brief description of the breach, including the date of the breach and the date of the discovery of the breach; (2) a description of the types of unsecured PHI involved in the breach; (3) steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of the actions taken by the covered entity to investigate the breach, to mitigate potential harm, and to protect against further breaches; and (5) steps that can be taken to obtain additional information.

Method of Notice: The notice must be provided by first-class mail to the individual at his or her last known address, or by electronic mail, if such method was previously agreed to by the individual. If the covered entity knows that the individual is deceased, written notice may be provided to the address of the next of kin or the individual’s personal representative.

Substitute Notice: If the covered entity has insufficient or out-of date contact information with respect to the covered individual, the covered entity must provide notice through alternative means. If insufficient or out-of-date information is available for fewer than 10 individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means. If insufficient or out-of-date information is available for 10 or more individuals, the covered entity must either post a conspicuous notice of the breach on the web site of the covered entity involved, or provide conspicuous notice in local major print or broadcast media. Such notice must include a toll-free telephone number where an individual can learn whether the individual’s unsecured PHI was included in the breach (the number must remain active for at least 90 days).

When is Media Notification Required?

In the case of breaches involving more than 500 residents of a State or jurisdiction, the covered entity must notify “prominent media outlets” of the State or jurisdiction. Such notice must be provided without unreasonable delay, and no later than 60 calendar days of the discovery of the breach, and must include the same content as described above with respect to the notification of individuals.

When is Notice Required to be Provided to HHS?

Breaches Involving 500 or more Individuals: For breaches involving 500 or more individuals, a covered entity must notify HHS of the breach at the same time notice is provided to the affected individuals as described above, and in the manner specified on the HHS web site (www.hhs.gov).

Breaches Involving Less than 500 Individuals: For breaches involving less than 500 individuals, a covered entity is required to maintain a log of such breaches and submit it to HHS on an annual basis. The log must be filed with HHS within 60 days after the end of the calendar year, and in the manner specified on the HHS web site (www.hhs.gov).

What Notification Requirements Apply to Business Associates?

Upon discovery of a breach, business associates are required to notify the covered entity of the breach without unreasonable delay, and no later than 60 calendar days after discovery of the breach. Such notice must include, to the extent possible, the identification of each affected individual as well as any other information that the covered entity is required to provide to the individual pursuant to the covered entity’s notice obligations.

As an exception to the notification requirements described above, the Final Rules allow covered entities to delay the notification of a breach if requested by a law enforcement official.

Recommended Action

The Final Rules require covered entities and business associates to take immediate steps to ensure compliance. Such steps include, among other things: (1) establishing internal procedures to determine when breaches of unsecured PHI have occurred and ensure

compliance with the notification requirements; (2) creating and maintaining a breach log to track any breaches so that they are properly reported to HHS; (3) training appropriate personnel on the notification requirements; (4) revising business associate agreements to account for the new requirements; and (5) modifying existing HIPAA policies and procedures and the notices of privacy practices to comply with the new notification requirements.

If you have any questions about this memorandum, please contact John C. Godsoe in our Buffalo office (716-566-2850, jgodsoe@bsk.com) or any of the other members of our Employee Benefits and Executive Compensation Practice Group listed below.

In Central New York, call 315-218-8000 or e-mail:

Susan L. Dahline	sdahline@bsk.com
Stephen C. Daley	sdaley@bsk.com
Brian K. Haynes	bhaynes@bsk.com
Richard D. Hole	rhole@bsk.com
Ted Lewkowicz	tlewkowicz@bsk.com
Aaron M. Pierce	apierce@bsk.com

In Buffalo / Niagara Falls call 716-566-2800 or e-mail:

Darcie A. Falsioni	dfalsioni@bsk.com
--------------------	--

In the Capital District, call 518-533-3000 or e-mail:

Amelia M. Klein	aklein@bsk.com
-----------------	--

On Long Island, call 516-267-6300 or e-mail:

Terry O'Neil	toneil@bsk.com
--------------	--

In New York City, call 646-253-2300 or e-mail:

Michael P. Collins	mcollins@bsk.com
--------------------	--

In the Rochester Region, call 585-362-4700 or e-mail:

Robert H. Kirchner	rkirchner@bsk.com
--------------------	--