



Employee Benefits Law Action Memo

April 2009

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

GUIDANCE ISSUED ON THE NEW HIPAA BREACH NOTIFICATION REQUIREMENTS

On April 17, 2009, the Department of Health and Human Services (“HHS”) issued guidance on what constitutes “unsecured protected health information” for purposes of the new breach notification requirements that will apply under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). These breach notification provisions will require, among other things, that covered entities (e.g., certain health plans, insurers, health care providers, and health care clearinghouses) notify individuals if their “unsecured protected health information” was used or disclosed in an unauthorized manner (as further defined below). Notices of such breaches also will have to be provided to the HHS and, in certain circumstances, to media outlets. Business associates of covered entities (e.g., certain third party administration, consulting, actuarial, legal, management, and financial services firms) also will be subject to certain breach notification requirements.

The HIPAA breach notification requirements were one of many significant new HIPAA privacy and security requirements that were included as part of the economic stimulus legislation that was enacted on February 17, 2009. Although most of these new HIPAA privacy and security requirements are not effective until February 17, 2010, the HIPAA breach notification requirements will be effective for breaches that are discovered on or after the 30th day following issuance of the applicable interim final regulations by the HHS (the HHS is required to issue those regulations by August 16, 2009). Entities that will be subject to the new HIPAA breach notification requirements should review the new HHS guidance on these requirements in order to help prepare for any required notices of breaches of “unsecured protected health information” that might occur later this year when the breach notification requirements become effective.

What Breaches of Protected Health Information Are Covered By the New Notification Requirements?

The new HIPAA breach notification requirements (“Breach Requirements”) only apply if there has been a “breach” of “unsecured protected health information.” Protected health information (“PHI”) is individually identifiable health information transmitted or maintained by a HIPAA covered entity or its business associates in any form or medium, and “unsecured” PHI (“Unsecured PHI”) is PHI that has not been secured through the use of a technology or methodology that has been approved by the HHS. The Breach Requirements apply to HIPAA covered entities and their business associates that, among other things, hold, use, or disclose Unsecured PHI.

A “breach” of Unsecured PHI occurs if, in general, there has been an unauthorized acquisition, access, use, or disclosure of Unsecured PHI which compromises the security or privacy of such information. However, a “breach” of Unsecured PHI will not be considered to have occurred if any of the following exceptions apply:

- if an unauthorized person to whom Unsecured PHI is disclosed would not reasonably have been able to retain such Unsecured PHI;
- if any unintentional acquisition, access or use of Unsecured PHI occurs by an employee or individual acting under the authority of a HIPAA covered entity or business associate, but only if (1) such acquisition, access or use was made in good faith and within the course and scope of the employment or other professional relationship with the covered entity or business associate, and (2) such Unsecured PHI is not further acquired, accessed, used, or disclosed; or



- where an inadvertent disclosure occurs by an individual who is otherwise authorized to access Unsecured PHI at a facility operated by a HIPAA covered entity or business associate to another similarly situated individual at the same facility, but only if the Unsecured PHI is not further acquired, accessed, used, or disclosed without authorization.

How Does the New HHS Guidance Define Unsecured PHI?

The new HHS guidance on the Breach Requirements (“HHS Guidance”) describes the technologies and methodologies that will make PHI unusable, unreadable, or indecipherable to unauthorized individuals. Proper use of such technologies and methodologies will help prevent PHI from becoming Unsecured PHI. Since the Breach Requirements only apply to Unsecured PHI, HIPAA covered entities and business associates can avoid having to comply with the Breach Requirements with respect to any PHI that is rendered unusable, unreadable, or indecipherable to unauthorized individuals in accordance with the HHS Guidance.

The HHS Guidance provides two methods for making PHI unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction. The HHS Guidance describes how these methods apply to the following data states:

- Data At Rest – An encryption process for “data at rest” (i.e., data that resides in databases, file systems, and other structured storage methods) will be valid if it is consistent with National Institute of Standards and Technology (“NIST”) Special Publication 800-111, *Guide To Storage Encryption Technologies for End User Devices*.
- Data In Motion – An encryption process for “data in motion” (i.e., data that is moving through a network, including wireless transmission) will be valid if it complies with the requirements of Federal Information Processing Standards (“FIPS”) 140-2.
- Data Disposed – “Data disposed” (e.g., discarded paper records or recycled electronic media) will be properly destroyed if (1) paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed, and (2) electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved.

The HHS Guidance is effective as of April 17, 2009. The HHS has asked for comments on a number of issues raised in the HHS Guidance, and modifications are possible when the interim final regulations are scheduled to be issued on or before August 16, 2009.

The HHS Guidance is only intended to be used to comply with the breach notification requirements described above, and does not relieve a HIPAA covered entity or business associate from the need to comply with other applicable PHI requirements, such as (1) a covered entity’s obligation to mitigate, to the extent practicable, any known harmful effect arising out of a breach of PHI by the covered entity or business associate, and (2) any other federal or state requirement that may apply following a breach of PHI (e.g., any state breach notification requirements).

How Must Notice of a Breach Be Provided?

If a HIPAA covered entity discovers a breach of Unsecured PHI, it must notify each individual whose Unsecured PHI has been, or is reasonably believed to have been, breached. If a business associate covered by HIPAA discovers such a breach, it must notify the covered entity about the individuals whose Unsecured PHI has been, or is reasonably believed to have been, breached. Such notices generally must be made without unreasonable delay, and in no event later than 60 calendar days after the breach is first discovered by the covered entity or business associate (subject to certain exceptions related to criminal investigations or national security matters).

Breach notices to individuals generally are required to be made by first-class mail (in certain circumstances, the notice can be done by electronic mail, telephone, conspicuous posting, and other specified methods). If a breach of Unsecured PHI affects, or is reasonably believed to affect, more than 500 residents of a particular state or jurisdiction, notice of that breach will have to be provided to prominent media outlets in that state or jurisdiction. Covered entities must notify the HHS immediately about breaches of Unsecured PHI involving more than 500 individuals, and annually for other breaches of Unsecured PHI. A posting will be made on an HHS web site of a list of each covered entity that has a breach of Unsecured PHI involving more than 500 individuals.

A notice of a breach of Unsecured PHI generally is required to include, among other things, (1) a description of the breach, (2) steps that affected individuals should take to protect themselves from potential harm that could arise out of the breach, (3) a summary of what the applicable covered entity is doing to investigate the breach, to mitigate potential losses, and to prevent additional breaches from occurring, and (4) steps that can be taken to obtain additional information.

If you have any questions about this memorandum, please contact Ted Lewkowicz in our Syracuse office (315-218-8131, tlewkowicz@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
Aaron M. Pierce	apierce@bsk.com

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

Darcie A. Falsioni	dfalsioni@bsk.com
John C. Godsoe	jgodsoe@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
--------------------	--