



# Employee Benefits Law Action Memo

March 2006

## Bond, Schoeneck & King, PLLC

### New York

Albany ■ 518-533-3000  
Buffalo ■ 716-566-2800  
Ithaca ■ 607-330-4000  
Long Island ■ 516-267-6300  
New York City ■ 646-253-2300  
Oswego ■ 315-343-9116  
Syracuse ■ 315-218-8000  
Utica ■ 315-738-1223

### Kansas

Overland Park ■ 913-234-4400

## Bond, Schoeneck & King, P.A.

### Florida

Bonita Springs ■ 239-390-5000  
Naples ■ 239-659-3800

## HIPAA ENFORCEMENT RULE EXPANDED AND FINALIZED; HIPAA SECURITY DEADLINE APPROACHING FOR SMALL GROUP HEALTH PLANS

### HIPAA Enforcement Rule Expanded and Finalized

On February 16, 2006, the Department of Health and Human Services ("HHS") issued final regulations addressing the enforcement of the Health Insurance Portability and Accountability Act ("HIPAA") administrative simplification provisions ("Enforcement Rule"). The final Enforcement Rule expands the application of the existing compliance and enforcement rules to all of HIPAA's administrative simplification provisions. (The compliance and enforcement rules previously covered only violations of the HIPAA privacy standards.) The Enforcement Rule is effective as of March 16, 2006.

#### Overview of the Enforcement Rule

Generally, the Enforcement Rule provides a vehicle for HHS to collect civil monetary penalties from covered entities who violate the HIPAA administrative simplification provisions. (The United States Department of Justice remains responsible for all criminal actions as a result of HIPAA violations; criminal actions are not affected by the Enforcement Rule.)

Under the Enforcement Rule, it is now mandatory for HHS to impose a civil monetary penalty if it is determined that a HIPAA violation has occurred. The Enforcement Rule outlines the factors that will be determinative in calculating the amount of the civil monetary penalty.

The following paragraphs provide a summary of some of the key points in the Enforcement Rule.

#### Compliance Reviews

Although HHS emphasizes that a covered entity should voluntarily comply with HIPAA, the final Enforcement Rule provides that the Secretary of HHS may conduct compliance reviews to

determine whether or not a covered entity is acting in accordance with the HIPAA administrative simplification rules. These compliance reviews are at the discretion of HHS.

#### Violations of Addressable Security Implementation Specifications

The HIPAA security provisions provide for "required" and "addressable" security implementation specifications. Although an "addressable" security implementation specification is not required, it must be implemented if it is determined to be reasonable and appropriate to implement. If a covered entity determines that it is not reasonable and appropriate to implement an addressable security implementation specification, the covered entity must document why it is not reasonable and appropriate. Further, the covered entity is required to implement an equivalent alternative measure if such alternative measure is reasonable and appropriate.

If a covered entity fails to (i) implement a reasonable and appropriate addressable standard, or (ii) document why it has determined that the addressable security implementation specification is not reasonable and appropriate, a violation of the HIPAA security rule will have occurred. In addition, a covered entity's failure to implement a reasonable and appropriate equivalent alternative measure is also a violation of the HIPAA security rule.

#### Covered Entity's Liability For Acts of Agents

Under the Enforcement Rule, a covered entity could be liable for certain violations of HIPAA by its agents (including business associates and work force members). As an exception, if a covered entity is in compliance with the HIPAA rules governing business associates (such as

*BS&K publications are for clients and friends of the firm and are not intended to substitute for professional counseling or advice.*

*For information about our firm, our practice areas and our attorneys, please visit our interactive web site, [www.bsk.com](http://www.bsk.com).*

© 2006 Bond, Schoeneck & King, PLLC  
All Rights Reserved

Printed on recycled paper

**BOND, SCHOENECK & KING, PLLC**  
ATTORNEYS AT LAW ■ NEW YORK FLORIDA KANSAS



entering into appropriate business associate agreements), the covered entity generally would not be liable for the actions of a business associate agent. (The federal law of agency will be used to determine whether the agent acted within the scope of its authority.)

#### Civil Monetary Penalty

While the final Enforcement Rule retains the provision under the proposed rule that imposes a penalty on a covered entity if a HIPAA violation occurs, the final Enforcement Rule eliminates the variables to be used by HHS in determining the number of HIPAA violations. Rather, the actual number of violations that occur will be determined by the nature of the covered entity's obligation to act or not act under HIPAA (such as an obligation to act in a certain manner, within a certain time, or with respect to a certain person). For continuing violations, for each day that a violation continues, a separate violation will have been deemed to have occurred. Generally, an act by a covered entity that violates overlapping subparts of HIPAA will be counted as one single violation, unless separate legal obligations exist.

With respect to the amount of a civil monetary penalty, HHS will take into account (i) the nature of the violation, (ii) the circumstances under which the violation occurred, (iii) the degree of culpability, (iv) the history of prior HIPAA violations, (v) the financial condition of the covered entity, and (vi) such other matters of justice as may be required. HHS will also consider mitigating factors.

A covered entity can challenge HHS's imposition of civil monetary penalties through hearings and an appellate review process.

#### **HIPAA Security Deadline Approaching For Small Plans**

The HIPAA security rule is the final part of the HIPAA administrative simplification requirements. It establishes the minimum standards for protecting the security of electronic protected health information ("ePHI") stored, maintained, created, received or transmitted by a covered entity via electronic media, including:

- e-mails;
- intranet or extranet;
- floppy disks;
- hard drives;
- magnetic tape; and
- electronic claims reports.

The deadline for compliance for small group health plans (plans with \$5 million or less in annual "receipts") is April 21, 2006. Large group health plans (plans with more than \$5 million in annual "receipts") were required to comply by April 21, 2005. (Annual "receipts" are the annual premiums paid for an insured plan, and the annual claims paid for a self-insured plan.)

In accordance with the HIPAA security rule, a group health plan must:

- ensure the confidentiality, integrity and availability of all ePHI;
- protect against any reasonably anticipated hazards or threats to the integrity or security of ePHI;

- protect against any reasonably anticipated impermissible uses or disclosures of ePHI; and
- ensure that the work force complies with the security requirements.

In order to satisfy the requirements set forth above, a covered entity must take the following steps to comply with the HIPAA security rule:

- a Security Official must be designated (this may be, but is not required to be, the same person designated as the Privacy Official);
- the group health plan must be amended to incorporate the security provisions;
- members of the work force must be trained with respect to the covered entity's security policies and procedures;
- business associate agreements must be updated to incorporate security provisions; and
- policies and procedures must be implemented to address security provisions, including –
  - (i) administrative safeguards for the business processes;
  - (ii) technical safeguards for the software and hardware; and
  - (iii) physical safeguards for the facilities and work space where ePHI is used and stored.

Some of the safeguards are "required" and some are "addressable." A covered entity must review each safeguard to determine whether it is reasonable and appropriate based upon the available financial resources, applicable budget considerations, the technical infrastructure, the security capabilities of the hardware and software, the costs of measures, and the risks to ePHI.

If you have any questions, please contact Darcie Falsioni (716-566-2862; [dfalsioni@bsk.com](mailto:dfalsioni@bsk.com)) or any of the other members of our Employee Benefits Law Practice Group listed below:

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

Lisa A. Christensen	<a href="mailto:lchristensen@bsk.com">lchristensen@bsk.com</a>
Stephen C. Daley	<a href="mailto:sdaley@bsk.com">sdaley@bsk.com</a>
Brian K. Haynes	<a href="mailto:bhaynes@bsk.com">bhaynes@bsk.com</a>
Richard D. Hole	<a href="mailto:rhole@bsk.com">rhole@bsk.com</a>
Ted Lewkowicz	<a href="mailto:tlewkowicz@bsk.com">tlewkowicz@bsk.com</a>
Aaron M. Pierce	<a href="mailto:apierce@bsk.com">apierce@bsk.com</a>

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

Joanmarie M. Dowling	<a href="mailto:jdowling@bsk.com">jdowling@bsk.com</a>
Amelia M. Klein	<a href="mailto:aklein@bsk.com">aklein@bsk.com</a>

*In Western New York, call 716-566-2800 or e-mail:*

John C. Godsoe	<a href="mailto:jgodsoe@bsk.com">jgodsoe@bsk.com</a>
----------------	--

In New York City and on Long Island, please contact any of the following members of our Labor and Employment Law Department:

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

Terry O'Neil	<a href="mailto:toneil@bsk.com">toneil@bsk.com</a>
--------------	--

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

Louis P. DiLorenzo	<a href="mailto:ldilorenzo@bsk.com">ldilorenzo@bsk.com</a>
--------------------	--