

IF YOU HAVE QUESTIONS REGARDING THIS MATTER, PLEASE CONTACT:



Kevin M. Wood
Associate, Austin
600 Congress Ave., Ste. 1600
Austin, Texas 78701- 2974
512-499-3664
kevin.wood@strasburger.com

EDITORS

Kathy Darling & David Bain

HEALTHCARE GROUP

David Andrew Bain
Virginia A. Barry
Debra W. Biehle
Thomas W. Burton
Renee Chafitz
Merritt M. Clements
Joseph F. Coniglio
Kathryn Midboe Darling
William Duane Darling
Rebecca L. Davis
R. Bradley Fletcher
Brian G. Hamilton
John R. Lowry
Bryan J. Maedgen
Cynthia Schafer Marietta
Stuart Miller
David G. Moore
Craig H. Myers
C. Scott Nichols
Laura Reilly O'Hara
Jeffrey S. Osgood
David L. Ovard
Donald Patrick Owens
Paul W. Sheldon
Layne Thompson
Joseph A. Turano
Melissa Webb
Carol D. Williamson
Ivan Wood
Kevin M. Wood

HIPAA: An Ever Present Compliance Concern

Since the Health Insurance Portability and Accountability Act ("HIPAA") was passed in 1996, various compliance issues have seemed ever present. One aspect of HIPAA compliance involves enforcement of HIPAA violations by the U.S. Department of Health & Human Services ("HHS"). The final HIPAA enforcement rules were published on February 16, 2006,¹ and became effective on March 16, 2006. In effect, the final enforcement rules extend the applicability of the Privacy Enforcement Rule to all of the HIPAA administrative simplification rules, including the Privacy Rule, the Security Rule, the Electronic Health Care Transactions and Code Set Standards, the Employer Identifier Standard, and the National Provider Identifier Standard. Collectively, the final HIPAA enforcement rules are referred to as the "Enforcement Rule."

The purposes of the Enforcement Rule are to clarify and elaborate on:

- The investigation process for alleged HIPAA violations;
- The bases for HIPAA liability in the event a violation is found;
- The determination of any civil monetary penalty ("CMP") amount;
- The grounds for waiver;
- The conduct of a hearing before an administrative law judge ("ALJ"); and
- The appeals process in the event a violation is deemed to have occurred.

To simplify and reduce the burden of HIPAA compliance for covered entities,² HHS adopted the Enforcement Rule to make the compliance and investigation provisions, which previously applied only to the Privacy Rule, applicable to all HIPAA rules and standards. By adopting this approach to enforcement, HHS has provided a cooperative approach to obtain HIPAA compliance, including the use of technical assistance and informal dispute resolution. The application of a single Enforcement Rule is further intended to simplify the process in the event a covered entity violates the provisions of more than one HIPAA rule or standard. HHS has also used the Enforcement Rule to clarify the manner in which investigations will be conducted, how testimony will be given, and how evidence obtained during an investigation may be used in a hearing or to determine the amount of any CMP.

Generally, a covered entity may incur CMP liability for the actions of an agent, including an employee, contractor, or volunteer, so long as the agent was acting within the scope of his or her agency. Please note that even though a business associate will often be an agent of a covered entity, a covered entity that complies with the HIPAA business associate requirements will generally not be held liable for HIPAA violations committed by the business associate.

The Enforcement Rule establishes maximum penalties of \$100 for each violation, up to \$25,000 per year for all violations of an identical HIPAA provision during the calendar year. This penalty cap is not a cap per covered entity, but is instead a

¹ See HIPAA Administrative Simplification: Enforcement; Final Rule, 71 Fed. Reg. 8390 (Feb. 16, 2006) (to be codified at 45 C.F.R. pts. 160 & 164).

² Covered entities are: (1) health plans; (2) health care clearinghouses; and (3) health care providers who transmit any health information in electronic form in connection with a HIPAA transaction.

cap per identical violation. For example, where a covered entity resells its used computers without scrubbing the hard drives that contain protected health information, this act may violate several separate legal obligations under the Privacy and Security Rules. Depending on the nature of the breaches, such violations could lead to consequential violations of other obligations. To the extent each of these violations can reach the \$25,000 cap, the \$25,000 penalty would be assessed for each violation, which could lead to a penalty assessment that totals hundreds of thousands of dollars.

Given the difficulty of determining the number of violations within a year, variables were proposed when calculating: (1) the number of disallowed activities (or failures to take required actions); (2) the number of persons involved or affected; and (3) the amount of time during which the violation occurred. The variable approach was rejected in the final rule, and the method for determining the actual number of violations will be based on the nature of the covered entity's obligation to act or not act under the provision that is alleged to have been violated. No minimum CMPs are established by the Enforcement Rule, but in determining the amount of any CMP, aggravating or mitigating factors will be considered.

Affirmative defenses to the imposition of a CMP are available. The Enforcement Rule provides some express affirmative defenses, but allows a respondent to offer other affirmative defenses than those listed. The listed affirmative defenses include: (1) the violation is otherwise a criminal offense and not subject to CMP liability; (2) lack of knowledge of the violation; and (3) the violation occurred due to reasonable cause, not willful neglect, and the covered entity corrected the violation within thirty (30) days of discovering the violation.

In an effort to minimize the possibility that different ALJs will decide similar issues differently, HHS had previously proposed an administrative review process for initial ALJ decisions to help achieve consistency in CMP determinations. The interim final CMP rule (issued April 17, 2003) made an ALJ decision the final decision of the Secretary of HHS. This allowed the respondent to file a petition for judicial review. The Enforcement Rule instead makes an ALJ decision the initial decision of the Secretary. Such a decision could then be appealed to the HHS Appeals Board within thirty (30) days of service of the ALJ's decision.

On a related note, the final compliance date for the HIPAA Security Rule is approaching. On April 20, 2006, small health plans must be in compliance with the Security Rule. All other covered entities, other than small health plans, were to be in compliance as of April 20, 2005. The Security Rule addresses three different categories: (1) administrative safeguards; (2) physical safeguards; and (3) technical safeguards. Thirteen of the security specifications are mandatory while the rest are "addressable," meaning that they are optional depending on the entity's costs and risk analyses, capabilities, current security measures, and other similar factors. From a practical standpoint, the policies and procedures that a covered entity can or should take are largely left to the discretion of the covered entity. The key is to remember that affirmative efforts must be taken by small health plans to achieve compliance with the Security Rule by April 20.