

Employee Benefits & Executive Compensation ADVISORY

April 1, 2009

Stimulus Act Imposes Increased HIPAA Obligation on Health Benefit Plans and Service Providers

The much-heralded economic stimulus package signed by President Obama on February 17, 2009 (ARRA or the "Act"),¹ dramatically expands and strengthens the security and privacy requirements under the Health Insurance Portability and Accountability Act of 1996 (the "HIPAA Rules"). Most of ARRA's security and privacy provisions will be effective within a year of ARRA's enactment; some provisions, however, are already in effect. This article highlights the key changes to the HIPAA Rules and the impact of these changes on health benefit plans, their business associates and certain previously non-covered entities.

Key Changes

Direct Regulation of Business Associates. Until now, the HIPAA Rules affected business associates (e.g., entities that provided services to health benefit plans, such as third party administrators, consultants, advisors, etc.) only indirectly by way of requiring the covered entity health plans to enter into a written agreement with each business associate, in order to obtain assurance of certain privacy and security safeguards. Under ARRA, the HIPAA Rules apply directly to the business associates, subjecting them to a broader array of requirements, direct regulatory oversight by the Department of Health and Human Services and substantially greater civil and criminal penalties for non-compliance.

Breach Notification Requirements. The breach notification provisions of ARRA will impose costly and burdensome requirements on covered entities and their business associates in the event of security or privacy breaches regarding protected health information (PHI).

Requirements for Other Types of Entities. Many entities not previously covered either as covered entities or business associates will now be subject to HIPAA's privacy and security compliance.

Additional Individual Privacy Rights. ARRA modifies and expands existing privacy rights for individuals under the HIPAA Rules. For example, it allows individuals who pay fully out-of-pocket for a health care service or item the right to have the claim not be submitted to their group health plan for payment or health care operations. Individuals will also have the right to request and receive information in an electronic format if it is maintained as an electronic health record (EHR). Individuals will also have the right to receive an accounting of PHI disclosures for treatment, payment and health care operations during the previous three years.

¹ American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (2009).

Strengthened Enforcement. The HIPAA Rules now provide state attorneys general with the authority to sue on behalf of individuals, along with the ability of individuals ultimately to obtain a portion of collected civil monetary penalties (CMPs).

Direct Regulation of Business Associates

Until ARRA, the HIPAA Rules regulated business associates only indirectly, by requiring covered entity health plans to enter into business associate agreements (BAAs) with their business associate service providers. These BAAs required the service providers to make certain assurances regarding the security and privacy of PHI they handle, and required the covered entities, if they become aware of a material breach or violation of the business associate agreement, to make reasonable efforts to remedy the situation, terminate the agreement or, if terminating the contract is not feasible, report the issue to the Secretary of the Department of Health and Human Services (the “Secretary of HHS”).

Under ARRA, the HIPAA Rules will apply directly to business associates in the same manner as those standards apply to covered entities. Likewise, the civil and criminal penalties for violating the privacy and security requirements of the HIPAA Rules and ARRA would also apply to business associates directly. Thus, business associates will be required to comply with most of the security requirements set forth in the HIPAA Rules as if they were covered entities like group health plans. In addition, the Secretary of HHS is required to issue annual guidance on the most effective and appropriate technical safeguards for protecting electronic health information, which must be taken into consideration by health plans and business associates alike.

The full implication of this direct application of the HIPAA Rules to business associates will not be clear until regulations are issued. Certain specifics, however, are already clear: business associates will be required to meet a broad range of the requirements currently applicable only to covered entities under the HIPAA Rules, such as obtaining individual authorization for certain uses and disclosures of PHI, establishing privacy and security policies and procedures, providing to individuals rights of access, amendment and entitlement to an accounting of disclosures, conducting a security risk assessment for electronic PHI and many of the other extensive requirements of the HIPAA Rules.

Business associates that are also covered entities (e.g., health plans and their affiliates) likely are already all too familiar with the direct requirements of the HIPAA Rules. Other business associates will have a great deal of legwork to ensure compliance with the new HIPAA Rule requirements.

Note: Business associates should not delay analyzing the full impact of this somewhat subtle change. The direct application of the HIPAA Rules will require a great deal of compliance activity for most entities. Steps should be undertaken now to begin the requisite risk assessment, implement HIPAA privacy and security policies and procedures, and otherwise ensure compliance with the full panoply of compliance obligations applicable under the HIPAA Rules.

Breach Notification Requirements

The HIPAA Rules currently do not specifically require health plans and other covered entities to notify individuals or the Secretary of HHS of a breach of the privacy, security or integrity of PHI. Further, business associates are only required to include in their business associate agreements a provision requiring them to report to the

covered entity the discovery of any security incident or any use or disclosure of PHI that is not addressed by their business associate agreement. ARRA, however, creates a new notification requirement for breaches of PHI that will have a significant impact on covered entities and business associates alike.

ARRA provides that, in the case of a breach with respect to unsecured PHI, the covered entity would be required to notify each individual whose information has been, or is reasonably believed to have been, accessed, acquired or disclosed as a result of such a breach. If the breach of PHI involves a business associate, the business associate is required to notify the covered entity. ARRA defines the term “breach” as the unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of such information. The definition, however, excludes certain inadvertent or unintentional disclosures, such as where one authorized user at a facility inadvertently discloses information to another authorized user at the same facility, so long as the information is not further acquired, accessed, used or disclosed without authorization. Thus, although the Act will broadly require that individuals be notified of breaches relating to their PHI, a covered entity would not necessarily be required to provide individual notification for every in-house breach of PHI. Still, this new notification requirement will be costly and burdensome, particularly where a breach involves the PHI of a large number of individuals.

In addition to notifying the individuals (which must be done not later than 60 days after discovery of the breach unless the notification would impede a criminal investigation or harm national security), covered entities also will be required to notify the Secretary of HHS of breach of PHI. If the breach involves 500 or more individuals, the notice to the Secretary of HHS must be immediate and the local media for the area where the individuals reside must also be notified. The Secretary of HHS is also required to post on the HHS Web site the list of covered entities involved in the breach of 500 or more individuals. In the case of breaches involving fewer than 500 individuals, the covered entity may maintain a log and annually submit such a log to the Secretary of HHS.

In implementing this requirement, the Secretary of HHS will provide interim final regulations within 180 days of February 17, 2009. Further, within 60 days of February 17, 2009, the Secretary of HHS will be responsible for issuing the first annual guidance on technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals (i.e., encryption).

Note: The new notification requirement constitutes a very significant change from current law. In addition to the cost burden associated with notifying all affected individuals, the requirement to notify the Secretary of HHS and the media can pose a significant negative public relations concern for covered entities. Because of these requirements, covered entities likely will be motivated to employ more extensive and expensive measures and technologies to safeguard PHI.

Requirements for Other Types of Entities

The current HIPAA provisions require only covered entities or business associates—and no others—to take mitigating actions (e.g., notify individuals in some cases) when their health information has been breached. Under ARRA, vendors of personal health records (PHRs) and other non-HIPAA-covered entities will also be required to notify individuals of breaches. This requirement expands HIPAA far beyond the previous scope of the HIPAA Rules, and demonstrates the new aggressive approach of Congress and the Obama administration toward protecting PHI.

Specifically, the Act requires that PHR vendors and certain non-HIPAA-covered entities (e.g., entities offering products and services through a PHR vendor's Web site), upon discovering a breach of security of "unsecured PHR identifiable health information," notify both the individuals affected by the breach and the Federal Trade Commission (FTC). The timeliness and content requirements that apply to covered entities and business associates with regard to such notifications also apply to these entities.

Note: The term "unsecured PHR identifiable health information" is PHR identifiable health information that is not protected through the use of a technology or methodology specified by the Secretary of HHS. In addition, third party service providers that provide services to PHR vendors and to certain other non-covered entities (e.g., entities offering products and services through a PHR vendor's Web site) that handle unsecured PHR identifiable health information are required to notify the vendor or other entity.

While the Secretary of HHS is to be notified by the FTC of any breaches, the FTC will have enforcement authority with regard to such breaches and will treat them as unfair and deceptive acts or practices in violation of the Federal Trade Commission Act. The FTC is required to issue interim final regulations with respect to these provisions within 180 days of February 17, 2009. Notably, the new privacy and security standards that apply under the Act to non-HIPAA-covered entities will be superseded by any new legislation enacted by Congress establishing breach notification requirements with respect to these entities.

Additional Individual Privacy Rights

ARRA modifies and expands existing privacy rights for individuals under the HIPAA Rules. Under the Act, individuals will have the right to request and receive their information in electronic format from a covered entity if such information is maintained as an electronic health record (EHR), and at a reasonable cost for complying with the request. With respect to requested restrictions on disclosures, covered entities such as medical providers will be required to restrict the disclosure of PHI to a health plan relating to an item or service for purposes of payment or health care operations if the individual has paid for such an item or service fully out-of-pocket. In addition, individuals will have the right to receive an accounting of PHI disclosures made by covered entities or their business associates for treatment, payment and health care operations during the previous three years. For current users of EHRs, this requirement will apply for disclosures made on or after January 1, 2014, and for non-users of EHRs, the later of January 1, 2011, or when the covered entity acquires EHRs. The Secretary of HHS also may impose a later effective date of not later than 2016 for current users, or not later than 2013 for non-users of EHRs.

Strengthened Penalty Provisions

Prior to the enactment of ARRA, the maximum civil monetary penalty (CMP) that may be imposed by the Secretary of HHS for violation of the privacy and security standards was \$100 per violation and up to \$25,000 for all similar violations within a given calendar year. CMPs may not be imposed for any of the following reasons: (1) the violation is a criminal offense under HIPAA criminal provisions; (2) the person did not have actual or constructive knowledge of the violation; or (3) the failure to comply was due to reasonable cause and not due to willful neglect, and the failure to comply was corrected within 30 days. With respect to certain wrongful disclosures of PHI, the Office of Civil Rights (OCR) may refer the case to the Department of Justice

for criminal prosecution. Criminal penalties under the HIPAA Rules include fines up to \$250,000 and up to 10 years in prison.

ARRA radically “ups the ante” for enforcement of civil violations under HIPAA in a number of consequential ways.

- First, the Act amends HIPAA to permit OCR to pursue an investigation and to impose CMPs against any individual for criminal violations of the HIPAA Rules if the Justice Department has not prosecuted the individual. That is, OCR will be permitted to impose CMPs even for violations that constitute a criminal offense, provided that the individual has not been prosecuted criminally.
- Second, the Act requires a formal investigation and imposition of CMPs for violations due to willful neglect. The Secretary of HHS is required to issue regulations within 18 months of ARRA enactment to carry out this change.
- Third, ARRA authorizes state attorneys general to bring a civil action in federal district court against individuals who violate the HIPAA Rules. The state attorneys general now will have this right of action either to enjoin violations or to seek damages of up to \$100 for each violation and \$25,000 for all similar violations within a calendar year.
- Fourth, the Act establishes four new tiers of CMPs, ranging from \$100 to \$50,000 for each violation, and \$25,000 to \$1,500,000 for similar violations within a calendar year. The tiers of CMPs would be based on the level of culpability, ranging from no knowledge of the violation to willful neglect. Thus, covered entities and business associates will be subject to considerable penalty amounts for violating the HIPAA Rules.
- Lastly, the Government Accountability Office (GAO) is tasked with recommending to the Secretary of HHS a methodology under which harmed individuals under HIPAA would receive a percentage of any CMP or monetary settlement collected with respect to a HIPAA violation. The Secretary of HHS, within three years of ARRA enactment, is required to establish by regulation (and based on GAO’s recommendations) the implementation of this methodology.

Together, these new and more severe sanctions, combined with enforcement authority by state attorneys general, will dramatically change the stakes for compliance with the HIPAA Rules.

If you would like to receive future *Employee Benefits and Executive Compensation Advisories* electronically, please forward your contact information including email address to employeebenefits.advisory@alston.com. Be sure to put “**subscribe**” in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Members of Alston & Bird’s Employee Benefits & Executive Compensation Group

Robert A. Bauman
202.756.3366
bob.bauman@alston.com

James S. Hutchinson
212.210.9552
jamie.hutchinson@alston.com

Andrea Prather
202.756.3354
andrea.prather@alston.com

Saul Ben-Meyer
212.210.9545
saul.ben-meyer@alston.com

Lindsay Jackson
202.756.3002
lindsay.jackson@alston.com

Nancy B. Pridgen
404.881.7884
nancy.pridgen@alston.com

Philip C. Cook
404.881.7491
philip.cook@alston.com

David C. Kaleda
202.756.3329
david.kaleda@alston.com

Thomas G. Schendt
202.756.3330
thomas.schendt@alston.com

Patrick C. DiCarlo
404.881.4512
pat.dicarlo@alston.com

Laurie Kirkwood
404.881.7832
laurie.kirkwood@alston.com

John B. Shannon
404.881.7466
john.shannon@alston.com

Ashley Gillihan
404.881.7390
ashley.gillihan@alston.com

Johann Lee
202.756.5574
johann.lee@alston.com

Maya D. Simmons
404.881.4601
maya.simmons@alston.com

David R. Godofsky
202.756.3392
david.godofsky@alston.com

Blake Calvin MacKay
404.881.4982
blake.mackay@alston.com

Carolyn E. Smith
202.756.3566
carolyn.smith@alston.com

Anna Grant
404.881.7124
anna.grant@alston.com

Emily W. Mao
202.756.3374
emily.mao@alston.com

Michael L. Stevens
404.881.7970
mike.stevens@alston.com

Anne Tyler Hamby
404.881.4839
annetyler.hamby@alston.com

Sean K. McMahan
404.881.4250
sean.mcmahan@alston.com

Laura G. Thatcher
404.881.7546
laura.thatcher@alston.com

Amy S. Heppner
404.881.7272
amy.heppner@alston.com

Michael G. Monnolly
404.881.7816
mike.monnolly@alston.com

Katherine A. Tritschler
404.881.7582
katie.tritschler@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Craig R. Pett
404.881.7469
craig.pett@alston.com

Kerry T. Wenzel
404.881.4983
kerry.wenzel@alston.com

H. Douglas Hinson
404.881.7590
doug.hinson@alston.com

ATLANTA

One Atlantic Center
1201 West Peachtree Street
Atlanta, GA 30309-3424
404.881.7000

CHARLOTTE

Bank of America Plaza
Suite 4000
101 South Tryon Street
Charlotte, NC 28280-4000
704.444.1000

DALLAS

Chase Tower
Suite 3601
2200 Ross Avenue
Dallas, TX 75201
214.922.3400

LOS ANGELES

333 South Hope Street
16th Floor
Los Angeles, CA 90071-3004
213.576.1000

NEW YORK

90 Park Avenue
New York, NY 10016-1387
212.210.9400

RESEARCH TRIANGLE

Suite 600
3201 Beechleaf Court
Raleigh, NC 27604-1062
919.862.2200

SILICON VALLEY

Two Palo Alto Square
Suite 400
3000 El Camino Real
Palo Alto, CA 94306-2112
650.838.2000

VENTURA COUNTY

Suite 215
2801 Townsgate Road
Westlake Village, CA 91361
805.497.9474

WASHINGTON, D.C.

The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202.756.3300

www.alston.com

© Alston & Bird LLP 2009