ALSTON&BIRD LLP

WWW.ALSTON.COM

Employee Benefits & Executive Compensation ADVISORY ■

MARCH 11, 2013

New HIPAA Omnibus Rule: Issues for Employer Plan Sponsors and Group Health Plans

HIPAA's long-awaited "Omnibus Rule" (also referred to in this advisory as the "Rule"), published on January 25, 2013, modifies numerous aspects of the HIPAA regulations concerning privacy, security, enforcement, and breach notification.[1] The Rule is effective on March 26, 2013, and requires compliance for most provisions by September 23, 2013. HHS has advised covered entities and business associates to update their policies and procedures and retrain workforce members, as appropriate, as a result of the changes implemented by the Omnibus Rule. While many of the changes are primarily applicable to health care providers, some action will also be required on the part of employer plan sponsors and their group health plans, as well as their business associates and subcontractors.

This advisory focuses on the Omnibus Rule provisions that most directly impact employer plan sponsors and group health plans. For a more thorough discussion of other sections of the Omnibus Rule, see the Alston & Bird Health Care Group's advisory published on January 25, 2013.[2] For a helpful general checklist on the new requirements, see the Alston & Bird Health Care Group's checklist published on February 1, 2013.[3]

This advisory is intended to help identify actions that employer plan sponsors and group health plans may need to take as a result of the Omnibus Rule. As discussed further in this advisory, the changes most significant for employer plan sponsors and group health plans include changes to the definition of business associate and breach; a more stringent enforcement scheme, including new rules regarding civil monetary penalties; modifications to the content of business associate agreements, notices of privacy practices and breach notifications; and implementation of the prohibition, under the Genetic Information Nondiscrimination Act (GINA), on use or disclosure of PHI that is genetic information for underwriting purposes.

---

1 Department of Health and Human Services, Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. The modifications implement the HIPAA amendments that took place under the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Nondiscrimination Act (GINA).

2 *Alston & Bird Health Care Advisory*, "Overview of HIPAA/HITECH Act Omnibus Final Rule," January 25, 2013, at http://www.alston.com/advisories/healthcare-HIPAA/HITECH-Act-Omnibus-FinalRule.

3 *Alston & Bird Health Care Advisory*, "HIPAA/HITECH Act Omnibus Rule Checklist," February 1, 2013, at http://www.alston.com/advisories/hipaa-hitech-omnibus-rule-checklist.

Expanded Business Associate Definition

The Omnibus Rule expanded the definition of business associate to include a variety of entities that have access to personal health records and other protected health information, such as patient safety organizations and health information organizations. While employer plans may not interact with all of these types of entities, it is important to be aware that many plan service providers (particularly those interacting with health care providers or insurers) will become business associates as a result of this rule.

In addition, under the Omnibus Rule, subcontractors that perform services for a business associate are themselves considered business associates to the extent their services involve the creation, receipt, maintenance or transmission of PHI on behalf of the business associate. Such subcontractor entities must obtain satisfactory assurances from their HIPAA-covered subcontractors (i.e., sub-subcontractors), in the form of a written agreement, that they will appropriately safeguard the PHI. If the entity only receives PHI to help the business associate with its own management, administration or legal responsibilities, it would not be considered a business associate. However, even in this situation, the business associate would need to obtain reasonable assurances from the subcontractor for the protection of PHI.

As discussed below (see *Numerous Changes to Privacy Rule*), the Omnibus Rule requires changes to most business associate agreements, and HHS has provided sample provisions for review and consideration in updating such agreements.[4]

More Stringent Enforcement Rule

In addition to significant changes to the business associate rules, the Omnibus Rule provides for a more stringent enforcement scheme. The Omnibus Rule now *requires* HHS to conduct an investigation and a compliance review in response to *any* complaint received if the facts indicate a possible violation due to willful neglect. In addition, the Omnibus Rule removed the requirement that HHS attempt an informal resolution of noncompliance (such as through demonstrated compliance or a completed corrective action plan). Therefore, following an investigation or a compliance review that indicates noncompliance, HHS can proceed directly to the use of civil monetary penalties (CMPs).

The Omnibus Rule also includes notable changes regarding CMPs. First, there is no longer an exception for liability of covered entities when HIPAA violations are committed by business associates acting as an agent of the covered entity. Covered entities are thus now liable for HIPAA violations by business associates if the business associate was acting (or failing to act) in its capacity as an agent of the covered entity. In determining whether a business associate is an agent, HHS follows the federal common law standard, which asks whether the covered entity had the right to control the agent's conduct. Generally, a business associate may be considered an agent if the business associate agreement with the covered entity grants the covered entity the authority to direct the performance of the service provided by the business associate after the relationship was established. Even where the business associate agreement does not provide the covered entity with such directive authority, an agency relationship may be found if the parties in fact behave as principal and agent. Business associates themselves face similar liabilities with respect to their subcontractors in the same manner as would covered entities with respect to business associates.

Practice Pointer: These changes to CMP liability could lead to potentially huge penalties for covered entities and business associates (each with respect to their business associate agents) through no action of their own, so it is crucial to ensure that any business associates who might qualify as agents follow the HIPAA rules.

---

[4] HHS, Sample Business Associate Agreement Provisions, January 25, 2013, at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

The Omnibus Rule provides, as did the 2009 interim final rule, for a tiered penalty scheme that ranges from $100 to $50,000 per occurrence, depending on the culpability of the covered entity or business associate, with a $1,500,000 maximum penalty for all identical violations during a calendar year. HHS has stated that it will not automatically issue the maximum penalty for every violation, and that the number of occurrences or violations would be determined based on context. The open-ended list of factors HHS will consider includes 1) the nature and extent of any violation, including the number of individuals affected and the relevant time period; 2) the nature and extent of any physical, financial or reputational harm, including any hindrance to the individual's ability to obtain health care; 3) any history of prior noncompliance; and 4) the financial condition and size of the covered entity or business associate. In the case of continuing violation of a HIPAA provision, however, a separate violation occurs each day the covered entity or business associate is in violation of the provision.

The penalty scheme is set forth in the following chart.

Category	Violation	Each Violation	Maximum for Identical Violations During a Calendar Year
Tier 1	Did Not Know	$100-$50,000	$1,500,000
Tier 2	Reasonable Cause	$1,000-$50,000	$1,500,000
Tier 3	Willful Neglect - Corrected	$10,000-$50,000	$1,500,000
	Willful Neglect - Not Corrected	$50,000	$1,500,000

The Rule also clarified the meaning of "reasonable cause," in Tier 2. "Reasonable cause" exists when the covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission is a violation, but did not act with the conscious intent associated with willful neglect.

Security Rule Applies to Business Associates

The Omnibus Rule revised HIPAA's Security Rule so it applies directly to business associates as well as to covered entities. Business associates, therefore, are now directly liable for Security Rule violations, and must 1) implement, review and update administrative safeguards (e.g., risk analysis and management, appointment of security official, training, etc.), physical safeguards (e.g., facility access controls, workstation use and security, device and media controls) and technical safeguards (e.g., access control, individual or entity authentication, transmission security, etc.); 2) obtain security-related written assurances from HIPAA-covered subcontractors by way of business associate agreements; 3) implement and maintain policies and procedures for compliance with the Security Rule; and 4) follow all documentation and maintenance requirements under the Security Rule.

In addition, the Omnibus Rule provides a new definition of electronic media to reflect technological advances. Electronic storage media, now known as "electronic storage material," explicitly includes intranets and voice transmissions that are electronically stored.

Numerous Changes to Privacy Rule

While certain Privacy Rule provisions will primarily affect providers, such as new definitions of health care operations and marketing and new rules about fundraising and the sale of PHI, others are relevant to all covered entities, including group health plans and their business associates.[5]

Privacy Rules Applicable to Business Associates

First, the Omnibus Rule extended the Privacy Rule's main obligations to business associates, including the prohibition on uses and disclosures of PHI except as permitted or required by the Privacy Rule; the requirement to restrict use or disclosure of, or request for, PHI to the minimum necessary to accomplish the intended purpose; the requirement to obtain and document written assurances (i.e., a business associate agreement) from business associates (or subcontractors, in the case of a business associate); and the threat of CMPs.

Second, the Omnibus Rule incorporated certain business associate agreement provisions into the Privacy Rule so that a business associate's violation of such provisions would constitute a Privacy Rule violation, as well as a contractual violation. Those provisions include, among others, the requirement to use or disclose PHI only in accordance with the business associate agreement or as required by law, the prohibition on use or disclosure of PHI in a manner that would be a Privacy Rule violation if done by the covered entity and the requirement to disclose PHI when required by the Secretary of HHS.

Third, the Omnibus Rule added requirements that apply to business associates, such as a requirement to disclose PHI as necessary to satisfy a covered entity's obligations relating to an individual's request for electronic PHI and prohibition against the sale of PHI. Other Privacy Rule requirements, such as the notice of privacy practices or the designation of a privacy official, do not apply to business associates unless the relevant contract requires them.

The Omnibus Rule also makes changes to various authorization rules, including those that make it easier to access the information of decedents. In addition, it permits providers who are not members of an employer's workforce but who provide health care to an individual at the request of an individual's employer to disclose PHI to the employer.

Contents of Business Associate Agreements

The Omnibus Rule modified the content requirement for business associate agreements. Specifically, it 1) eliminates the requirement that covered entities report to the Secretary of HHS when it is not feasible to terminate a business associate agreement; 2) requires a business associate that is aware of noncompliance by a subcontractor to respond appropriately; 3) adds several new requirements for business associates;[6] and 4) where a business associate carries out a covered entity's obligation, requires the business associate to comply with the relevant rules. The Omnibus Rule allows for a transition period in which compliant business associate agreements that are in effect prior to January 25, 2013, and not renewed or modified from March 26, 2013, until September 23, 2013, are deemed to be compliant until the earlier of the date they are renewed or modified or September 22, 2014.

---

[5] If your covered entity does engage in marketing or activities which would constitute the sale of PHI, see a detailed explanation of the new rules in the *Health Care Group Advisory* at http://www.alston.com/advisories/healthcare-HIPAA/HITECH-Act-Omnibus-FinalRule.

[6] These include complying with the applicable Security Rule provisions if it handles electronic PHI; reporting breaches of unsecured PHI to the covered entity; and ensuring that any subcontractors that create or receive PHI on its behalf agree to the same restrictions with respect to such information as apply to the business associate.

Practice Pointer: If you do not have business associate agreements in place, or have business associate agreements in place prior to January 25, 2013, that are not compliant with HIPAA requirements, the deadline for having business associate agreements that comply with the Omnibus Rule is September 23, 2013. For business associate agreements in place prior to January 25, 2013, that are compliant with HIPAA requirements, *and so long as they are not modified or renewed from March 26, 2013, until September 23, 2013*, the deadline for having business associate agreements that comply with the Omnibus Rule is the earlier of September 22, 2014, or the date the business associate agreement is modified or renewed. If your business associate agreements do not need to be amended, be sure not to accidentally trigger compliance with the new rules by renewing or modifying them before it is necessary to do so.

In connection with the revised business associate agreement content requirements, HHS provided sample business associate agreement provisions on its website, including language for definitions, the obligations and activities of a business associate, permitted uses and disclosures by a business associate, provisions for the covered entity to inform the business associate of privacy practices and restrictions, permissible requests by the covered entity, and term and termination of the contract.

Practice Pointer: This is sample language, and using it is not required for compliance. However, it is a helpful guide in developing or updating Business Associate Agreements that would satisfy HHS scrutiny. Covered entities and business associates should follow the language closely, but tailor it to the specific needs of their business.

Notice of Privacy Practices

The Omnibus Rule significantly modified the content requirements for notices of privacy practices (NPPs). In addition to existing content requirements, NPPs must now provide 1) that authorization is required for most uses and disclosures of psychotherapy notes, uses and disclosures of PHI for marketing purposes and disclosures that constitute a sale of PHI; 2) opt-out rules if a covered entity intends to contact the individual for fundraising purposes; 3) for health plans (other than long-term care policy issuer) that intend to use or disclose PHI for underwriting purpose, that the covered entity cannot use or disclose genetic information for such purposes; 4) a statement of the rights of affected individuals to be notified following a breach of unsecured PHI; and 5) a statement that a covered entity must agree to an individual's request for restriction on disclosure of PHI to a health plan if the disclosure is for payment or health care operations purposes and pertains solely to a health care item or service for which the covered entity has been paid in full by a person other than the health plan. HHS specifically notes that these modifications constitute material changes to NPPs, triggering distribution obligations for covered entities.

The Omnibus Rule also includes altered distribution requirements for NPPs. A health plan that currently posts its NPP on its website must (1) prominently post the material change or its revised NPP on its website by the effective date of the material change to the NPP and (2) provide, in the next annual mailing, the revised NPP or information about the material change and how to obtain the revised NPP. If a health plan does not have a customer service website, it must provide the revised NPP, or information about the material change and how to obtain the revised NPP, to its covered individuals within 60 days of revision. Plans should provide both paper- and web-based notices to be accessible to all beneficiaries, including those with disabilities. Finally, as long as the required contents are present, the covered entity may utilize a layered notice, or a short notice with a longer notice attached.

Practice Pointer: All covered entities, including all health plans, must have new NPPs posted by September 23, 2013, so it is important to begin working on an updated NPP soon.

The Omnibus Rule also expanded individual access rights to PHI maintained electronically, whether or not the designated record set is an "electronic health record." If an individual requests an electronic copy of PHI that is maintained electronically in a designated record set, the covered entity must provide access in the form and format requested, or in another agreed-upon format. Also, as required to be disclosed in NPPs, providers must comply with requests to restrict disclosures to health plans if the disclosure is for payment or health care operations and the PHI relates only to an item or service for which the individual (or anyone other than the health plan) has paid in full. The Omnibus Rule also includes new provisions about disclosures to third parties, reasonable fees and timeliness of response.

Changes to Breach Determination and Notification Requirements

Generally, "breach" is defined as the impermissible acquisition, access, use or disclosure of PHI that compromises the security or privacy of PHI. The Omnibus Rule modified the definition of "breach" by removing the requirement to determine the occurrence of a breach by assessing whether the impermissible acquisition, access, use or disclosure poses a "significant risk of financial, reputational, or other harm" to the individual. In its place, the Omnibus Rule installed a rebuttable presumption—where there is an impermissible acquisition, access, use or disclosure of PHI, a breach is presumed unless the covered entity or business associate demonstrates, through a risk assessment, that there is a low probability that PHI has been compromised. The risk assessment must consider at least the following factors: 1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; 2) the unauthorized person who used the PHI or to whom the disclosure was made; 3) whether the PHI was actually acquired or viewed; and 4) the extent to which the risk to the PHI has been mitigated. Entities may consider other factors, but the analysis must be thorough and in good faith, and it must reach a reasonable conclusion. In addition, covered entities and business associates can provide breach notifications following any impermissible use or disclosure without performing a risk assessment, if they choose to do so.

As set forth in the HITECH Act and now codified in the Privacy Rule, the required breach notice has several content requirements.[7] It must include 1) a brief description of the event, 2) a description of the types of unsecured PHI involved, 3) steps individuals should take to protect themselves, 4) a brief description of steps taken by the covered entity and 5) contact information. The notification must be provided by first-class mail, or electronic mail if agreed to by the individual. In the event there is insufficient or out-of-date information for providing the notice by mail, the Omnibus Rule provides parameters for a substitute method of notice that is reasonably calculated to reach the individual. There is a 60-day outer limit in which covered entities or business associates must fulfill the individual notification requirements.

Covered entities are responsible for notifying affected individuals of a breach. If they choose to delegate this responsibility to a business associate, the two entities should evaluate which is in the best position to do so. Importantly, HHS has confirmed that when a business associate is acting as an agent of the covered entity, its discovery of the breach will be attributed to the covered entity; as a result, the covered entity is required to provide notification at this point, not when they are notified. If the business associate is not an agent, however, the covered entity's time for notification begins to run based on the time it is notified of the breach. HHS encourages covered entities and business associates to address the timing of notifications in their business associate agreements.

---

7 These requirements do not differ from those published in the 2009 Interim Final Rule.

Practice Pointer: Because breach discovery[8] by agents is treated as breach discovery by the covered entity or the business associate (as applicable), it is important to have procedures for efficient reporting by agents so that the covered entity can have more time to investigate and inform affected individuals as necessary.

The preamble to the Omnibus Rule also provided clarifications regarding breach notifications to prominent media outlets, which is required if more than 500 individuals in one state or jurisdiction are affected by a breach. A press release on the covered entity's website would not fulfill the obligation to provide notice to the media. While the entity must directly provide notice to the media, it is not required to incur any cost to run a notice, and the media outlet is not obligated to print or run any information about the breach. In addition, with regard to required notification to the Secretary of HHS for breaches involving less than 500 individuals, the Secretary must be notified no later than 60 days after the end of the calendar year in which the breaches were *discovered* (not the year in which they occurred).

The Omnibus Rule also eliminated the breach exception for limited data sets that exclude dates of birth and zip codes. This change is significant for employers that currently communicate through limited data set exchanges that are not encrypted. Also, HHS clarified that the Office of Civil Rights (OCR) may impose CMPs against those entities failing to comply with the breach notification requirements. OCR also has the authority to work with covered entities to achieve voluntary compliance, except in cases involving willful neglect.

Provisions Required by Genetic Information Nondiscrimination Act (GINA)

The Omnibus Rule implements the changes required by GINA by prohibiting all health plans, except for long-term care policy insurers, from using or disclosing an individual's PHI *that is genetic information* for underwriting purposes. This rule applies to all genetic information from the compliance date of the Rule, regardless of when or where it originated. In addition, it applies to health plans that are covered entities under the HIPAA privacy rule, including those to which GINA does not expressly apply.

GINA amended the definition of "health information" to include "genetic information," which is defined as 1) an individual's genetic tests; 2) genetic tests of family members of such individual; 3) manifestation of a disease/disorder in family members of such individual; or 4) any request for, receipt of, genetic services or participation in clinical research that includes genetic services by such individual or a family member. The Omnibus Rule adopts this definition under GINA, along with other related definitions under GINA (for terms such as "family member," "genetic services" and "genetic test") without modification.

How Should You Respond?

Now is the time to make sure that your documents, policies and procedures, training material, and relationships with any business associates are compliant with the new rules. For a helpful general checklist on the new requirements, see the Alston & Bird Health Care Group's checklist, published on February 1, 2013.[9]

***This advisory was written by* Johann Lee, Stacy Clark *and* John Hickman.**

---

[8] A breach is considered discovered as of the first day on which such breach is known to the covered entity (or its agent) *or, by exercising reasonable diligence, would have been known to the covered entity (or its agent)*.

[9] *Alston & Bird Health Care Advisory*, "HIPAA/HITECH Act Omnibus Rule Checklist," February 1, 2013, at http://www.alston.com/advisories/hipaa-hitech-omnibus-rule-checklist.

If you would like to receive future *Employee Benefits & Executive Compensation Advisories* electronically, please forward your contact information 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
202.239.3366
bob.bauman@alston.com

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

Stacy C. Clark
404.881.7897
stacy.clark@alston.com

Emily Seymour Costin
202.239.3695
emily.costin@alston.com

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

Ashley Gillihan
404.881.7390
ashley.gillihan@alston.com

David R. Godofsky
202.239.3392
david.godofsky@alston.com

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

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

Emily C. Hootkins
404.881.4601
emily.hootkins@alston.com

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

Johann Lee
202.239.3574
johann.lee@alston.com

Blake Calvin MacKay
404.881.4982
blake.mackay@alston.com

Emily W. Mao
202.239.3374
emily.mao@alston.com

Douglas J. McClintock
212.210.9474
douglas.mcclintock@alston.com

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

Earl Pomeroy
202.239.3835
earl.pomeroy@alston.com

Jonathan G. Rose
202.239.3693
jonathan.rose@alston.com

Syed Fahad Saghir
202.239.3220
fahad.saghir@alston.com

Thomas G. Schendt
202.239.3330
thomas.schendt@alston.com

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

Richard S. Siegel
202.239.3696
richard.siegel@alston.com

Carolyn E. Smith
202.239.3566
carolyn.smith@alston.com

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

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

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

Elizabeth Vaughan
404.881.4965
beth.vaughan@alston.com

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

Kyle R. Woods
404.881.7525
kyle.woods@alston.com

ALSTON&BIRD LLP

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213-576-1100
NEW YORK: 90 Park Avenue ■ 12th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 275 Middlefield Road ■ Suite 150 ■ Menlo Park, California, USA, 94025-4004 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.756.3300 ■ Fax: 202.756.3333
VENTURA COUNTY: 2801 Townsgate Road ■ Suite 215 ■ Westlake Village, California, USA, 91361 ■ 805.497.9474 ■ Fax: 805.497.8804