

Employee Benefits & Executive Compensation ADVISORY

September 9, 2009

Life's a Breach: What Constitutes a Breach under the HIPAA HiTech Breach Notification Requirements

On August 24, 2009, the Department of Health and Human Services (HHS) published in the Federal Register its interim final rule (the "Breach Regulations") requiring notification of breaches of unsecured protected health information (PHI) by covered entities and their business associates under the Health Insurance Portability and Accountability Act (HIPAA).¹ The Breach Regulations² follow on the heels of HHS' guidance issued in April 2009 (which was incorporated into the Breach Regulations) that established the manner in which covered entities and business associates may secure PHI (the "Encryption Guidance")³ and ultimately avoid the notice obligations set forth in the Breach Regulations. These new requirements apply to breaches *occurring* on or after September 23, 2009. HHS has indicated that it will not impose sanctions for failure to provide the required notifications for breaches that are discovered before February 22, 2010; however, HHS expects HIPAA-covered entities to comply with the Breach Regulations during this initial time period and will work with entities through technical assistance and voluntary corrective action to achieve compliance.

This advisory focuses on identifying a breach and whether possible exceptions apply. Our prior advisory (accessible at http://www.alston.com/healthcare_advisory_HHS_breach_notification) provides more information on other aspects of the Breach Regulations (such as the notice requirements).⁴

Practice Pointer: Although business associates and covered entities have slightly different notice obligations, each must be able to identify "breaches" in order to satisfy its respective notice obligations.

¹ 74 Federal Register 42740 (August 24, 2009).

² These regulations will be codified in Subpart D to Part 164 of Title 45 of the Code of Federal Regulations.

³ 74 Fed. Reg. 19006 (April 27, 2009).

⁴ The Breach Regulations, HITECH and the Encryption Regulations shall be collectively referred to herein as the "Breach Notification Rules." References to the Security Rules mean 45 CFR part 164, Subparts A and C, and references to the Privacy Rules mean 45 CFR part 164, Subparts A and E.

Brief Overview

- **Breach Defined.** The Breach Regulations provide a specific definition of “breach” for purposes of the notice obligations set forth in the Breach Regulations. Compliance with the Breach Regulations hinges on understanding this definition and being able to identify “breaches.” A “breach” for purposes of the Breach Regulations and the corresponding notice obligation occurs only if (i) there is an acquisition, access, use or disclosure (ii) of unsecured PHI (iii) that violates the HIPAA Privacy Rules⁵ relating to use and disclosure of PHI and (iv) that compromises the security or privacy of the unsecured PHI. The definition of “breach” has several moving parts and exceptions, and thus requires careful examination. Not every violation of the HIPAA Privacy Rules will constitute a breach for purposes of the Breach Regulations.
- **“Unsecured” PHI.** The specific notice obligations set forth in the Breach Regulations arise only for breaches of “unsecured” PHI. PHI is “secured” for purposes of the Breach Regulations only to the extent the Encryption Guidance is satisfied. If the PHI is secured in accordance with the Encryption Guidance, then the specific notice obligations set forth in the Breach Regulations do not apply—even if there is an unauthorized use or disclosure of PHI (although other notice obligations may apply).
- **Compromised PHI.** Even if unsecured PHI is used or disclosed in a manner that violates HIPAA’s Privacy Rules, it is not a “breach” for purposes of the Breach Regulations if the violation does not “compromise the security or privacy” of the PHI. PHI is compromised to the extent it “*poses a significant risk of financial, reputational, or other harm to the individual.*” Each time there is an unauthorized use or disclosure of unsecured PHI, covered entities must conduct a risk assessment to determine if the breach poses a significant risk of harm to the individual. The Breach Regulations identify several factors that may be considered when conducting the risk assessment.
- **Burden of Proof.** Covered entities have the burden of demonstrating that they satisfied the specific notice obligations following a “breach” as defined by the Breach Regulations or, if notice is not made following an unauthorized use or disclosure, that the unauthorized use or disclosure did not constitute a “breach.”

Practice Pointer: Plan sponsors must reevaluate and revise their existing HIPAA privacy policies and procedures to ensure compliance with the new Breach Regulations. See “Action Plan for Compliance” below for a more detailed discussion.

What is a “Breach” for Purposes of the Breach Notification Rules?

The specific notice obligations set forth in the Breach Regulations apply only to the extent there has been a “breach” as defined by the Breach Regulations. The Breach Regulations define a “breach” as “the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of [45 CFR part 164] ⁶ which compromises the security or privacy of protected health information, except where an

⁵ Generally, the privacy rules include subparts A and E of 45 CFR § 160 and 164; the Breach Regulations apply only to impermissible uses or disclosures under subpart E of 45 CFR § 164.

⁶ Generally, the privacy rules include subparts A and E of 45 CFR § 160 and 164; the Regulations apply only to impermissible uses or disclosures under subpart E of 45 CFR § 164.

unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.” This definition has several moving parts and requires careful examination. Practically speaking, unless otherwise specifically excepted, a breach contains the following elements:

- an acquisition, access use or disclosure
- of “unsecured” PHI
- that violates HIPAA’s Privacy Rules relating to use or disclosure of PHI and
- that compromises the security or privacy of such PHI.

These elements and the specific exceptions are discussed in more detail below.

PHI Only. As a threshold matter, the Breach Regulations are concerned only with breaches involving PHI. If the information is not PHI, there is no breach. Thus, de-identified information⁷ and employment records held by a covered entity in its role as employer⁸ are not PHI. On the other hand, limited data sets are considered PHI and are generally subject to the Breach Regulations; however, the Breach Regulations provide a narrow exception for certain limited data sets that also exclude both birth dates and zip codes (see below for a more detailed discussion of the narrow exception).

Acquisition, access, use or disclosure. To be a breach, there must be an “acquisition, access, use or disclosure” of unsecured PHI. These terms are broadly defined and encompass essentially any access, use or exchange of PHI (whether authorized or not). Although the regulations do not specifically define “acquisition and access,” HHS noted in the preamble to the Breach Regulations that it interprets the terms based on their plain meanings, and that each is encompassed within the current definitions of “use” and “disclosure.” “Use” is currently defined as the “sharing, employment, application, utilization, examination, or analysis of [PHI] within an entity that maintains such information.”⁹ Disclosure is currently defined as the “release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information”¹⁰

Practice Pointer: A mere use or disclosure of PHI does not trigger a breach analysis if (i) the use or disclosure is impermissible under HIPAA or (ii) the use or disclosure is subject to an exception. See “HIPAA Privacy Rule Violation” and “Specific Exceptions” below for more detail.

“Unsecured” PHI. Only an acquisition, access, use or disclosure of “unsecured” PHI can constitute a “breach” for purposes of the Breach Regulations and the corresponding notice obligations. “Unsecured” PHI is PHI that is not secured through the use of encryption or destruction that renders the PHI unusable, unreadable or indecipherable to unauthorized individuals. Only PHI secured in accordance with the Encryption Guidance is considered “unusable, unreadable, or indecipherable” for purposes of the Breach Regulations.

⁷ 45 CFR 164.514(b).

⁸ 45 CFR 160.103.

⁹ 45 CFR 160.103.

¹⁰ 45 CFR 160.103.

The Encryption Guidance. According to the Encryption Guidance, PHI is considered unusable, unreadable or indecipherable to unauthorized individuals if it has been encrypted by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key,”¹¹ and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools must be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The Encryption Guidance identifies specific methods that HHS has determined, in accordance with statute, meet the standard. (See our prior advisory on the Encryption Guidance, accessible at http://www.alston.com/health_care_advisory_recovery.)

Practice Pointer: Access controls do not meet the standard set forth in the Encryption Guidance for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals. Thus, PHI that is accessible only to those who have an authorized password is not “secure” under the Encryption Guidance.

Therefore, if a covered entity “secures” PHI in accordance with the Encryption Guidance, and an unauthorized use or disclosure is discovered, the specific notice obligations set forth in the Breach Regulations do not apply because the PHI is considered “secure” and, thus, there is no breach. On the other hand, if some other method not specifically identified in the Encryption Guidance is used, then the PHI is not considered secure and an unauthorized use or disclosure may constitute a “breach,” giving rise to the specific notice obligations set forth in the Breach Regulations.

Practice Pointer: HHS has emphasized that Encryption Guidance does nothing to modify a covered entity’s responsibilities with respect to the Security Rule, nor does it impose any new requirements upon covered entities to encrypt all PHI. A covered entity may be in compliance with the Security Rule even if it reasonably decides not to “secure” PHI in accordance with the Encryption Guidance and instead uses a comparable method to safeguard the information.

Violation of HIPAA Privacy Rules. An acquisition, access, use or disclosure of unsecured PHI will not give rise to a “breach” unless the acquisition, access, use or disclosure is a violation of HIPAA’s Privacy Rules. For example, a disclosure of PHI that violates the minimum necessary rule may constitute a “breach” under the Breach Regulations to the extent the other “breach” elements exist (e.g., the PHI is unsecured and the disclosure compromises the security of the PHI). Fortunately, a breach may only arise to the extent HIPAA’s Privacy Rules are violated. A violation of the Security Rule does not itself constitute a potential breach under the Breach Regulations, although such a violation may lead to a use or disclosure of PHI that is not permitted under the Privacy Rule and may potentially be a breach.

Practice Pointer: A violation of HIPAA’s Privacy Rules will not rise to the level of a “breach” unless the rule violated relates to use and disclosure of PHI. Thus, a violation of HIPAA’s administrative safeguards does not, in and of itself, give rise to a “breach,” but, much like a violation of the Security Rule, such a violation may lead to a breach.

¹¹ 45 CFR 164.304, definition of “encryption.”

Compromise the Security or Privacy of PHI. Even if it is established that a use or disclosure of unsecured PHI violates the Privacy Rule, a breach may not have occurred if the violation does not “compromise the security or privacy” of the PHI. The Breach Regulations clarify that this means that the use or disclosure “poses a significant risk of financial, reputational, or other harm to the individual.” Consequently, covered entities and business associates will need to perform a risk assessment each time there is an unauthorized use or disclosure to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. In performing the risk assessment, HHS identified a non-exhaustive list of factors¹² for covered entities and business associates to consider:

- (1) ***Who impermissibly used the information and to whom was the information impermissibly disclosed?*** HHS states that if, for example, PHI is impermissibly disclosed to another entity governed by the HIPAA Privacy and Security Rules, or to a federal agency that is obligated to comply with the Privacy Act of 1974 (5 USC 552a) and the Federal Information Security Management Act of 2002 (44 USC 3541 et seq.), there may be less risk of harm to the individual, because the recipient entity is obligated to protect the privacy and security of the information it received in the same or similar manner as the entity that disclosed the information. In contrast, if PHI is impermissibly disclosed to any entity or person that does not have similar obligations to maintain the privacy and security of the information, the risk of harm to the individual is much greater. Other guidance recommended by HHS adds that the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others may also be a consideration.¹³
- (2) ***Whether any immediate steps have been taken to mitigate an impermissible use or disclosure.*** HHS provides by way of example that obtaining the PHI recipient’s “satisfactory assurances” that the PHI will not be further used or disclosed (through a confidentiality agreement or similar means), or will be destroyed, may eliminate or reduce the risk of harm to the individual to a less than “significant risk.” Consequently, no breach will have occurred.
- (3) ***Whether the PHI disclosed was returned prior to being accessed.*** There may be circumstances where impermissibly disclosed PHI is returned prior to it being accessed for an improper purpose. For example, if a laptop is lost or stolen and then recovered, and a forensic analysis of the computer shows that its information was not opened, altered, transferred, or otherwise compromised, HHS states that such a breach may not pose a significant risk of harm to the individuals whose information was on the laptop. Note, however, that if a computer is lost or stolen, HHS does not consider it reasonable to delay breach notification based on the hope that the computer will be recovered.
- (4) ***The type and amount of PHI involved in the disclosure.*** In performing a risk assessment, covered entities and business associates should also consider the type and amount of PHI involved in the impermissible use or disclosure. If the nature of the PHI does not pose a significant risk of financial, reputational or other harm, then the violation is not a breach. As an example, HHS provides that, if a covered entity improperly discloses PHI that “merely” includes the name

¹² These factors and examples are listed in the preamble to the Regulations, pages 42744-42745, and are not in the actual Regulations.

¹³ OMB Memorandum M-07-16.

of an individual and the fact that he received services from a hospital, this disclosure may not constitute a significant risk of financial or reputational harm to the individual, even though it would constitute a violation of the Privacy Rule. If, however, the information indicates the *type* of services that the individual received, or that the individual received services from a specialized facility (such as a substance abuse treatment program), or if the PHI includes information that increases the risk of identity theft (such as a social security number, account number or mother's maiden name), then there is a higher likelihood that the impermissible use or disclosure compromised the security and privacy of the information.

- (5) ***The risk of re-identification of PHI contained in a limited data set.***¹⁴ As explained below, HHS provides a narrow, explicit exception for limited data sets that exclude both birth dates and zip code information; if, however, either one of those elements is included, a risk assessment must be performed. HHS cites an example whereby an impermissible use or disclosure of a limited data set that includes zip codes, based on the population features of those zip codes, may not create a significant risk that a particular individual can be identified. If there is no significant risk of harm to the individual, then no breach has occurred and no notification is required. If, however, the risk assessment reveals that the individual can be identified based on the information disclosed, and there is otherwise a significant risk of harm to the individual, then breach notification is required (unless one of the other exceptions discussed applies).

HHS also notes that factors from OMB Memorandum M-07-16 may also be used in the risk assessment. Although those factors are similar to the factors described above, the OMB memo notes that harm to reputation, as well as “the potential for harassment or prejudice,” should be considered, and cautions that notification when there is little or no risk of harm might create unnecessary concern and confusion.

Are There Any Exceptions to the Rule?

HHS has provided four exceptions to the definition of a “breach.” Consistent with the statute, the Breach Regulations indicate the following unauthorized uses or disclosures of unsecured PHI are not considered a “breach” for purposes of the Breach Regulations:

- (1) *Any unintentional acquisition, access, or use of PHI by a workforce member¹⁵ or person acting under the authority of a covered entity or business associate, if the acquisition, access, or use was made in good faith and within the scope of the person's duties and does not result in further use or disclosure in violation of the Privacy Rule.*

The Breach Regulations modified the statutory language from “employees” to “workforce members.” A workforce member means “employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.”¹⁶ A person is acting under the “authority” of a covered

¹⁴ Limited data set is defined at 45 CFR § 164.514(e) of the Privacy Rule.

¹⁵ A “workforce member” includes employees, volunteers, trainees and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. See 45 C.F.R. § 160.103.

¹⁶ 45 CFR § 160.103.

entity or business associate if he or she is acting on its behalf in accordance with common law agency principles. This may include a workforce member of a covered entity, an employee of a business associate or even a business associate of a covered entity. Similarly, to determine whether the access, acquisition or use was made “within the scope of authority,” the covered entity or business associate should consider whether the person was acting on its behalf at the time of the inadvertent acquisition, access or use.

Additionally, while the statutory language provides that this exception applies where the recipient does not further use or disclose the information, HHS interprets this exception as encompassing circumstances where the recipient does not further use or disclose the information in a manner *not permitted under the Privacy Rule*. In circumstances where any further use or disclosure of the information *is* permissible under the Privacy Rule, there is no breach solely because of the further use or disclosure.

- (2) *Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, or business associate, or organized health care arrangement in which the covered entity participates, and the information is not further used or disclosed in violation of the Privacy Rule.*

The Breach Regulations modify the statutory language slightly to except from the definition of “breach” inadvertent disclosures of PHI from a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate or organized health care arrangement in which the covered entity participates.

HHS also clarifies that “similarly situated individual” as used in the statute with regard to this second exception means an individual who is authorized to access PHI, even if that individual is not authorized to access the PHI at issue. For example, a physician who has authority to use or disclose PHI at a hospital by virtue of participating in an organized health care arrangement with the hospital is similarly situated to a nurse or billing employee at the hospital. In contrast, the physician is not similarly situated to an employee at the hospital who is not authorized to access PHI.

Additionally, HHS clarifies that “same facility” as used in the statute with regard to this second exception means the same covered entity, business associate or organized health care arrangement in which the covered entity participates, even if at a different location. Thus, if a covered entity has a single location, then the exception will apply to disclosures between a workforce member and, for example, a physician with staff privileges at that single location. However, if a covered entity has multiple locations across the country, the same exception will apply even if the workforce member makes the disclosure to a physician with staff privileges at a facility located in another state.

- (3) *A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.*

HHS has modified the statutory language to except from the definition of “breach” situations where a covered entity or business associate has a good faith belief that the unauthorized person would not reasonably have been able to retain the information.

Example 1: A covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. In these circumstances, the covered entity can conclude that the improper addressees could not reasonably have retained the information. The EOBs that were not returned as undeliverable, however, and that the covered entity knows were sent to the wrong individuals, should be treated as potential breaches.

Example 2: A nurse mistakenly hands a patient the discharge papers belonging to another patient, but she quickly realizes her mistake and recovers the PHI from the patient. If the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, then this would not constitute a breach.

- (4) *An acquisition, access, use or disclosure of PHI involving a limited data set that excludes both birth dates and zip code information.*

A limited data set is created by removing the 16 direct identifiers from the PHI.¹⁷ When these 16 direct identifiers are removed from PHI, the information is not completely de-identified under the Privacy Rule. In particular, the elements of dates, such as dates of birth, and zip codes are allowed to remain within the limited data set, which increase the potential for re-identification of the information. Under the Breach Regulations, an unauthorized use or disclosure of a limited data set does not rise to the level of a “breach,” to the extent that it excludes birth dates and zip codes. If, however, the limited data set does contain either birth dates or zip code information, then this narrow exception would not apply and the covered entity would have to perform the breach analysis with respect to the use or disclosure of the limited data set, *including the risk assessment described above*. HHS has cautioned that this narrow exception should not be construed as encouraging or permitting the use or disclosure of more than the minimum necessary information.¹⁸ HHS has invited comments on this narrow exception.

Practice Pointer: As noted in more detail below, if the covered entity does not send notice in reliance on one of these exceptions, the covered entity is responsible for documenting the facts supporting the determination that an exception applied.

¹⁷ A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers or household members of the individual: (1) names; (2) postal address information, other than town or city, state and zip code; (3) telephone numbers; (4) fax numbers; (5) e-mail addresses; (6) social security numbers; (7) medical record numbers; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate/ license plate numbers; (11) vehicle identifiers and serial numbers; (12) device identifiers and serial numbers; (13) Web URLs; (14) Internet Protocol (IP) address numbers; (15) biometric identifiers, including finger and voice prints; and (16) full face photographic images and any comparable images.

¹⁸ As set forth in 45 CFR §§ 164.502(b) and 164.514(d).

Are Any Changes to Our Privacy Policies and Procedures Required?

The Breach Regulations require covered entities to comply with the administrative requirements of certain provisions of the Privacy Rule¹⁹ with respect to the breach notification provisions. These provisions, for example, require covered entities and business associates to develop and document policies and procedures, train workforce members on and have sanctions for failure to comply with these policies and procedures, permit individuals to file complaints regarding these policies and procedures or a failure to comply with them, and require covered entities to refrain from intimidating or retaliatory acts. Thus, a covered entity is required to consider and incorporate the requirements of the Breach Notification Rules with respect to its administrative compliance and other obligations.

Who Has the Burden of Proof of Compliance?

Covered entities and business associates have the burden of proof that they have satisfied their respective notice obligations under the Breach Regulations. Thus, in the event of a “breach”, the covered entity must be able to prove that it notified affected individuals, the media and HHS as required. Likewise, business associates must be able to prove that they notified covered entities of any breaches. If notice is not provided following an unauthorized use or disclosure, then the covered entity or business associate must be able to prove that the unauthorized use or disclosure was not a breach. Accordingly, when a covered entity or business associate knows of an impermissible use or disclosure of PHI, it should maintain documentation that all required notifications were made, or, alternatively, of its risk assessment or the application of any exceptions to the definition of “breach,” to demonstrate that notification was not required. For impermissible uses or disclosures of PHI that fall under the narrow exception for limited data sets that do not include zip codes or dater of birth, documentation that demonstrates that the lost information did not include these identifiers will suffice.

What Are the Next Steps for Plan Sponsors and Business Associates?

September 23 is right around the corner, and even with the non-enforcement policy announced by HHS, February 22 seems ominous. Plan sponsors and their business associates should implement an action plan and quickly take steps to ensure compliance. Note: For additional details on the breach notice requirements, see our prior advisory at: http://www.alston.com/healthcare_advisory_HHS_breach_notification.

- **Establish Breach Identification Procedures.** Covered entities and business associates will need to implement procedures for identifying when a breach has occurred that should include the following steps:
 - Determine whether there has been an impermissible use or disclosure of PHI under the Privacy Rule.
 - If the PHI does not fit into the narrow exception for certain limited data sets, undertake a risk assessment by determining, and documenting, whether the impermissible use or disclosure compromises the security or privacy of the PHI in a manner that poses a significant risk of financial, reputational, or other harm to the individual.
 - Determine whether the incident falls under one of the three statutory exceptions to the breach definition.

¹⁹ Specifically, § 164.530(b), (d), (e), (g), (h), (i) and (j).

- **Establish Breach Notification Procedures.** Covered entities and business associates should determine which breach notification must be sent (i.e., individual notices, substitute notices, urgent notices, immediate notices to HHS, media notices, notice from business associate to covered entity) and who will be responsible for gathering the necessary information for such notification, preparing the notices, and sending the notices.
- **Document Breaches for HHS Reporting.** For breaches of unsecured PHI involving fewer than 500 individuals, a covered entity must maintain a log or other documentation of such breaches, and notify HHS not later than 60 days after the end of each calendar year about breaches occurring during the preceding calendar year (details to be provided on the HHS web site).
- **Amend Business Associate Agreement.** Covered entities and business associates should coordinate their breach notification efforts in order to avoid duplicate notices and to ensure efficiency with regard to information gathering and time frames. Covered entities whose business associates act as agents of the covered entity should consider requiring business associates to notify the covered entity of a breach discovery well in advance of the 60-day deadline provided in the Breach Regulations, as the breach discovery date of the business associate/agent shall be treated as the breach discovery date for the covered entity for purposes of providing a timely notice to individuals and, if required, HHS and the media.
- **Workforce Training.** The clock for sending breach notifications begins to tick as soon as a breach is known (or, by exercising reasonable diligence, would have been known) to *any workforce member or agent* (other than the person committing the breach) of the covered entity. Covered entities and business associates will want to enhance training so that their employees are aware of the importance of timely reporting of privacy and security incidents, and of the consequences of failing to do so.
- **Administrative Requirements—Revise Policies and Procedures, Training, Sanctions, Complaint Process.** Covered entities must incorporate the requirements of the Breach Regulations into their policies and procedures, and workforce training sanctions for failure to comply must be developed, as well as a complaint process for failures to comply with these new policies and procedures.

Covered entities and business associates should consult legal counsel to work through these steps to ensure that breach notification is provided when required.²⁰

²⁰ The Breach Regulations, HITECH and the Encryption Regulations shall be collectively referred to herein as the “Breach Notification Rules.” References to the Security Rules mean 45 CFR part 164, Subparts A and C, and references to the Privacy Rules mean 45 CFR part 164, Subparts A and E.

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

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

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

Lindsay Jackson
202.756.3002
lindsay.jackson@alston.com

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

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

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

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

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

Laurie Kirkwood
404.881.7832
laurie.kirkwood@alston.com

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

Ashley Gillihan
404.881.7390
ashley.gillihan@alston.com

Johann Lee
202.756.5574
johann.lee@alston.com

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

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

Blake Calvin MacKay
404.881.4982
blake.mackay@alston.com

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

Anna Grant
404.881.7124
anna.grant@alston.com

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

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

Anne Tyler Hamby
404.881.4839
annetyler.hamby@alston.com

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

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

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

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

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

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

Craig R. Pett
404.881.7469
craig.pett@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