



EMPLOYEE BENEFITS CLIENT ALERT

April 9, 2009

RECOVERY ACT CHANGES TO HIPAA PRIVACY AND SECURITY

On February 17, 2009, the President signed the American Recovery and Reinvestment Act (the "Recovery Act"). Among other things, the Recovery Act revises and extends the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

BACKGROUND

HIPAA created national standards for the protection of individuals' health information (known as "protected health information" or "PHI"). HIPAA also established certain individual rights concerning PHI. Regulations implementing HIPAA—particularly the provisions known as the Privacy Rule and the Security Rule—elaborate on the protections that health care providers, health care clearinghouses and health plans ("Covered Entities") must follow.

In the Recovery Act, Congress expanded both HIPAA and the government's power to enforce HIPAA. This Client Alert addresses some of the more significant changes to HIPAA brought about by the Recovery Act.

BUSINESS ASSOCIATES

Under HIPAA, the term "Business Associate" refers to a person (other than an employee) or company that provides services to or on behalf of a Covered Entity, if the person or company needs access to PHI to perform the services. Prior to the Recovery Act, Business Associates were not directly regulated by HIPAA. Instead, Business Associates were required to sign agreements with Covered Entities whereby the Business Associates promised to abide by certain HIPAA standards.

Under the Recovery Act, Business Associates are subject to HIPAA's provisions directly. Like Covered Entities, Business Associates may be prosecuted for criminal violations of the Privacy Rule and the Security Rule and can be subject to civil money penalties as well.

As a result of the Recovery Act, by February 17, 2010, Business Associates must take a number of significant steps:

- Business Associates must adopt administrative, physical and technical safeguards that meet the requirements of the Security Rule.
- Business Associates must have written policies and procedures that meet the requirements of the Privacy Rule and the Security Rule.
- Business Associate agreements must be amended to reflect the expanded responsibilities of the Business Associates.

In addition, the Recovery Act specifies that "Business Associate" includes any entity that provides data transmission of PHI for a Covered Entity and requires access to PHI on a routine basis, such as: a Health

Information Exchange Organization, a Regional Health Information Organization, or an E-prescribing Gateway.

NOTIFICATION OF BREACH

Under HIPAA, a breach of security or privacy generally did not have to be reported to the individual or to the government. The Recovery Act imposes significant notification requirements for certain breaches. Although there are a few exceptions, the general rule is that a “breach” occurs when there is an unauthorized use, disclosure, access or acquisition of “unsecured PHI.” By August 16, 2009, the Department of Health and Human Services (“HHS”) must publish proposed regulations for making PHI “secured.” The notification rules will apply to any breach discovered more than 30 days after the proposed rules are published.

Highlights of the notification rules include:

- *Notification to Covered Entity.* If a Business Associate discovers a breach, the Business Associate is required to report the breach to the Covered Entity without unreasonable delay and within 60 days after the breach.
- *Notification to Individuals.* A Covered Entity must notify each individual whose PHI was breached. Notification must occur without unreasonable delay and within 60 days after the breach. If the Covered Entity does not have sufficient information to contact 10 or more individuals whose PHI was breached, the Covered Entity must post a conspicuous notice of the breach on its Web site or must provide the notice to major print or broadcast media outlets in the area where the individuals affected by the breach likely reside. In all cases of breach affecting more than 500 residents of a state or jurisdiction, notice shall be provided to prominent media outlets serving such state or jurisdiction.
- *Notification to HHS.* If the breach involves PHI belonging to 500 or more individuals, the Covered Entity must notify HHS immediately. If the breach involves fewer than 500 individuals, the Covered Entity must include the breach in an annual report to HHS.
- *Content of Notification.* Among other things, the notice must include the steps that individuals should take to protect themselves from further harm. The notice also must explain how the Covered Entity is repairing damage caused by the breach and how it is protecting against similar breaches in the future.

Vendors of personal health records (and related entities) are not always Covered Entities and may not be subject to HIPAA. Nevertheless, under the Recovery Act, these vendors must follow notification rules that are nearly identical to the above. The primary difference is that breaches are reported to the Federal Trade Commission instead of HHS.

EXPANDED ENFORCEMENT

To date, the Privacy Rule has been enforced by HHS and the Security Rule has been enforced by the Centers for Medicare and Medicaid Services (“CMS”). Each Agency continues to have the power to audit and to impose civil money penalties. The Recovery Act expanded HIPAA’s enforcement scheme in a number of ways:



- State attorneys general have the power to bring a civil action when they believe that someone within their jurisdiction has been injured by a HIPAA violation.
- Civil penalties are currently available only upon a “knowing” violation of HIPAA. Under the Recovery Act, civil penalties are available if a HIPAA violation is due to “willful neglect,” “reasonable cause,” or even if the violator “did not know” that he or she was violating HIPAA. The Recovery Act includes separate penalty levels for each of these different levels of culpability.
- CMS and HHS are required to perform audits and investigate complaints.

INDIVIDUAL RIGHTS

The Recovery Act expanded individuals’ rights in a number of ways:

- *Right to Request Restrictions.* Individuals have the right to ask a Covered Entity not to use or disclose their PHI in certain ways. Under the Recovery Act, a Covered Entity must agree to the request if it relates to certain types of disclosures by a provider to a health plan.
- *Right to an Accounting.* Individuals have the right to ask a Covered Entity for an accounting of the instances in which the Covered Entity has disclosed the individual’s PHI.
 - The accounting covers the previous six-year period and may omit certain disclosures, such as disclosures for treatment purposes. Under the Recovery Act, if the accounting relates to an “electronic health record,” the accounting covers only the previous three years, but the accounting may not omit any disclosures.
 - Covered Entities have been responsible for collecting the accounting information from their Business Associates and presenting it to the individual as requested. Under the Recovery Act, a Covered Entity may provide the individual with a list of the appropriate Business Associates. If the individual contacts a Business Associate and requests an accounting, the Business Associate must respond directly to the individual.
- *Right to Access.* Under the Recovery Act, if a Covered Entity maintains an electronic health record on an individual, the individual has a right to obtain a copy of the records in electronic format.

MISCELLANEOUS

Sales. The Recovery Act largely restricts the sale of PHI. There are a number of exceptions. For example, the exceptions allow sales to the individual, sales authorized by the individual, and sales made as part of the merger or acquisition of the business entity that maintains the PHI.

Minimum Necessary. In most circumstances HIPAA requires that Covered Entities and Business Associates use and disclose only the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure. (The minimum necessary rule does not apply to disclosure for purposes of treatment.) Congress instructed HHS to issue more specific guidance as to the meaning of “minimum necessary” by August 17, 2010.

De-identified Information. HIPAA allows Covered Entities and Business Associates to freely disclose “de-identified” PHI. Essentially, this means that the PHI has been stripped of all identifiers that could reasonably be used to link the medical information to the individual. Congress has instructed HHS to provide specific guidance as to the acceptable methods of de-identifying PHI by February 17, 2010.



HOW KUTAK ROCK CAN HELP

As always, we are available to assist you with all aspects of HIPAA—answering one-time questions, managing a full-scale compliance program, and anything in between. In particular:

- *If you are a Covered Entity*, we can help identify Business Associates, review and revise your Business Associate agreements, update your policies and procedures to accommodate the expansion of individual rights, and develop processes for complying with the notification rules.
- *If you are a Business Associate*, we can help develop the privacy and security policies, procedures and forms that you will need by mid-February. We can also review and update your Business Associate agreements.

For more information on the material contained in this Client Alert, contact your regular Kutak Rock representative or any member of our Employee Benefits practice group listed below. For more information on our Employee Benefits and Executive Compensation practice and for recent news and alerts, please visit us at www.kutakrock.com.



John E. Schembari
john.schembari@kutakrock.com



Peter C. Langdon
peter.langdon@kutakrock.com



Janis J. Winterhof
janis.winterhof@kutakrock.com



Juliana Reno
juliana.reno@kutakrock.com



Michelle M. Ueding
michelle.ueding@kutakrock.com



Kathryn M. Magli
kathryn.magli@kutakrock.com



William C. McCartney
william.mccartney@kutakrock.com



Margaret A. Olsen
margaret.olsen@kutakrock.com

Kutak Rock LLP | The Omaha Building | 1650 Farnam Street | Omaha, NE 68102-2186 | (402) 346-6000

This Employee Benefits Client Alert is a publication of Kutak Rock LLP. This publication is intended to notify our clients and friends of current events and to provide general information about employee benefits issues. The Kutak Rock LLP Employee Benefits Client Alert is not intended, nor should it be used, as legal advice, and it does not create an attorney-client relationship.

To ensure compliance with requirements imposed by the IRS, we inform you that any federal tax advice contained in this communication should not be used or referred to in the promoting, marketing or recommending of any entity, investment plan or arrangement, and such advice is not intended or written to be used, and cannot be used, by a taxpayer for the purpose of avoiding penalties under the Internal Revenue Code.

©Kutak Rock LLP 2009
All Rights Reserved

This communication may be considered advertising in some jurisdictions.



Atlanta • Chicago • Denver • Des Moines • Fayetteville • Irvine
Kansas City • Little Rock • Los Angeles • Oklahoma City • Omaha • Philadelphia
Richmond • Scottsdale • Washington, D.C. • Wichita

NATIONAL RESOURCES, LOCAL RESULTS™