



EMPLOYEE BENEFITS CLIENT ALERT

August 25, 2009

NOTICE OF BREACH: HHS ISSUES NEW HIPAA REGULATIONS

In 1996 the Health Insurance Portability and Accountability Act (“HIPAA”) created national standards for the protection of individually identifiable health information (“protected health information” or “PHI”) by health care providers, health care clearinghouses and health plans (“Covered Entities”). Earlier this year, HIPAA was amended by the American Recovery and Reinvestment Act. Among other things, the recent amendments extended many of HIPAA’s requirements directly to the contractors (“Business Associates”) of Covered Entities. We issued a [previous Client Alert summarizing these amendments](#).

Under the recent amendments, Covered Entities and Business Associates must provide certain notices when there is a “breach” of “unsecured” PHI. Yesterday, the Department of Health and Human Services (“HHS”) published interim final regulations in the Federal Register, providing guidance concerning the notice and breach issues. Below, we outline the items of greatest significance to our clients.

WHAT CONSTITUTES A “BREACH”?

As amended, HIPAA defines a “breach” as the use or disclosure of PHI that is “unauthorized” and that “compromises the privacy or security” of PHI. In the new regulations, HHS clarifies these terms.

- An “unauthorized” use or disclosure is one that violates HIPAA’s privacy rule. It is important to note that not every violation of the privacy rule is a breach—only violations which involve uses and disclosures are breaches. It is also important to note that a violation of the *security* rule does not constitute a breach and does not require notice.
- To “compromise the privacy or security” of PHI means to “pose a significant risk of financial, reputational, or other harm to the individual.” Where an unauthorized use or disclosure occurs, Covered Entities and Business Associates are expected to conduct a fact-specific risk assessment that considers all relevant factors, which may include: the person or entity who improperly used the PHI or to whom the PHI was improperly disclosed; whether steps were taken that mitigated the improper use or disclosure; and the type and amount of PHI involved. The risk assessment should be documented so that the Covered Entity or Business Associate can demonstrate, if necessary, that no breach occurred and no notification was necessary.

WHAT IS “UNSECURED” PHI?

Covered Entities and Business Associates must safeguard the privacy and security of PHI. If the PHI is “secured,” then a breach of the PHI does not require notice. HHS has issued guidance that outlines the permissible methods of “securing” PHI (e.g., encryption), and will update this guidance on its Web site at <http://www.hhs.gov/ocr/privacy>.

WHAT NOTICE IS REQUIRED?

When there has been a breach of unsecured PHI, a Covered Entity must notify HHS and the individuals whose PHI was breached. In some cases, the Covered Entity must notify the media. If a Business Associate discovers the breach, the Business Associate must notify the Covered Entity. The new regulations specify the timing, content and manner of notice. Of particular interest:

KUTAK ROCK LLP

- Notice to the individual (or by a Business Associate to a Covered Entity) must be made “without unreasonable delay” and in no event more than 60 days after the breach is “discovered.” A breach is “discovered” on the first day that the breach would have been known if the Covered Entity and the Business Associate exercised the “business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.”
- If the breach involves 500 or more individuals, the Covered Entity’s notice to HHS must be made at the same time as the notice to the individual.
- If the breach involves fewer than 500 individuals, the Covered Entity’s notice to HHS must be included on an annual submission, which is due no later than 60 days after the end of the calendar year.

IMPORTANT DATES

The new regulations apply to breaches of unsecured PHI that occur on or after **September 23, 2009**. HHS recognizes that it will take Covered Entities and Business Associates time to implement the new regulations. As such, HHS has announced that for breaches discovered before **February 22, 2010**, the failure to provide a timely notice generally will not result in sanctions. However, Covered Entities and Business Associates are expected to comply with the new regulations and still will be required to take corrective action.

ACTION ITEMS

Covered Entities and Business Associates should promptly begin developing policies and procedures that:

- Implement reasonable systems for discovering, reporting and investigating breaches.
- Ensure that workforce members are adequately trained concerning the importance of reporting breaches.
- Govern the drafting, approval and issuance of the required notices.
- Protect those who report and investigate breaches and prevent retaliation against such persons.
- Require adequate documentation of the breach, from discovery through notice.

The new regulations, together with their preamble, are over 100 pages long. Of necessity, this Client Alert has only touched on a few of the key issues. 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](#)
[Michelle M. Ueding](#)

[Peter C. Langdon](#)
[Kathryn M. Magli](#)

[Janis J. Winterhof](#)
[William C. McCartney](#)

[Juliana Reno](#)
[Margaret A. Olsen](#)

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.



NATIONAL RESOURCES, LOCAL RESULTS™