



*Independent Insurance Agents*

*Brokers of America, Inc.*



## **OFFICE OF THE GENERAL COUNSEL**

### **HIPAA BREACH NOTIFICATION RULE**

This memorandum is not intended to provide specific advice about individual legal, business or other questions. It was prepared solely as a guide, and is not a recommendation that a particular course of action be followed. If specific legal or other expert advice is required or desired, the services of an appropriate, competent professional should be sought.

September 23, 2009

#### **Introduction**

As part of the American Recovery and Reinvestment Act of 2009, the U.S. Department of Health and Human Services (“HHS”) published the “Breach Notification Rule,” which supplements regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The Breach Notification Rule requires notice when there is a breach by entities covered by HIPAA (“Covered Entities”), or by business associates of Covered Entities (“Business Associates”), of unsecured protected health information that causes a significant risk of harm to the affected individuals.

The Breach Notification Rule became effective September 23, 2009, but the HHS will not impose sanctions for failure to give notice of breaches discovered (or that reasonably should have been discovered) through February 22, 2010.

This memorandum provides an overview of what independent insurance agents and brokers that are Covered Entities or Business Associates must do to comply with the requirements of the Breach Notification Rule, and how such agents and brokers can shield themselves from the notification requirements.

#### **The Breach Notification Rule**

The Breach Notification Rule requires Covered Entities and Business Associates to provide notice when there is a “breach” of “unsecured” protected health information (“PHI”), and the breach “compromises the security” of the PHI. With respect to Covered Entities and Business Associates, PHI is health information that can identify individuals and that is transmitted or maintained in written, oral, electronic or any other form.

## Elements of the Breach Notification Rule

Notice is not required under the Breach Notification Rule unless *all three* of the following elements exist.

(1) There is a “breach” of PHI:

A breach occurs when there is unauthorized acquisition, access, use or disclosure of PHI.

(2) The PHI is “unsecured”:

PHI is considered unsecured when it is not protected using the methods described in HHS’s guidelines for securing and destroying data under the Health Information Technology for Economic and Clinical Health Act (“HITECH”). As a result, agents and brokers that are Covered Entities or Business Associates that comply with the HITECH guidelines get safe harbor protection and are not required to provide notification in the event of such a breach. Although Business Associates and Covered Entities do not have to follow the HITECH guidelines to be in compliance with HIPAA, the benefit of the safe harbor is a compelling reason to comply with the guidelines. The HITECH guidelines describe methods for encrypting electronic data (such as the use of TLS and VPNs), storing and destroying electronic data, and destroying physical records. More information about the HITECH guidelines is available at: <http://www.hhs.gov/ocr/privacy> and <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf>.

(3) The breach “compromises the security” of the PHI:

In order to trigger the Breach Notification Rule’s notification requirement, the breach must “compromise the security” of the PHI, which means the breach must cause a significant risk of financial, reputational or other harm to the affected individual. Agents and brokers subject to the Breach Notification Rule will need to perform a risk assessment to determine if there is a significant risk of harm due to a breach, based on factors such as (i) who received the information without authorization, (ii) the type and amount of PHI impermissibly disclosed or used, and (iii) what, if any, steps were taken to mitigate the harm.

## Exceptions to the Breach Notification Rule

There are three exceptions to when unauthorized acquisition or disclosure of PHI will be deemed a “breach,” so that notice will not be required under the Breach Notification Rule. The exceptions are:

- (1) Unintentional acquisition, access or use of PHI by an employee or individual acting under the authority of a Covered Entity or Business Associate;

- (2) Inadvertent disclosure of PHI from one person authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the Covered Entity or Business Associate; and
- (3) Unauthorized disclosure in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

#### Notice Required by Business Associates

If a Business Associate discovers (or reasonably should have discovered) a breach of unsecured PHI that compromises the security of the PHI, the Breach Notification Rule requires the Business Associate to notify the Covered Entity without unreasonable delay, and in any event within 60 days. The business associate contract between the Covered Entity and the Business Associate may require an even shorter notice period. If a Business Associate has PHI from more than one Covered Entity and it is unclear whose information has been breached, the Business Associate may need to provide notice to all potentially affected Covered Entities.

#### Notice Required by Covered Entities

If a Covered Entity discovers (or reasonably should have discovered) a breach of unsecured PHI that compromises the security of the PHI, the Breach Notification Rule requires the Covered Entity to notify each affected individual without unreasonable delay, and in any event within 60 days.

In cases affecting more than 500 individuals, the Covered Entity also must provide notice to HHS.

If more than 500 individuals *in the same state or jurisdiction* are affected, notice must be provided to prominent media outlets serving the state or jurisdiction. Such notice may be in the form of a press release. For the purpose of the Breach Notification Rule, the term “jurisdiction” means a geographic area smaller than a state, such as a county, city or town. Notice to the media, if required, is to be provided in addition to notices to HHS and the affected individuals.

If a Business Associate is an *independent contractor* of a Covered Entity, then the Covered Entity’s time period to provide notice will be triggered by when the Business Associate notifies the Covered Entity of the breach (assuming the Covered Entity does not discover, or reasonably should have discovered, the breach earlier). If a Business Associate is an *agent* of a Covered Entity, however, then the date the Business Associate discovers a breach of PHI will be deemed the date the Covered Entity discovered the breach. For this reason, Covered Entities may decide to add shorter notice periods for Business Associates in their business associate contracts.

## Relationship to State Laws

The Breach Notification Rule is in addition to any state-law requirements and preempts any contrary state laws, so agents and brokers should continue to comply with any additional state-law requirements that are not contrary to the Breach Notification Rule. According to HHS, “a state law is contrary if ‘a covered entity could find it impossible to comply with both the State and federal requirements’ or if the State law ‘stands as an obstacle to the accomplishment and execution of the full purposes and objectives’ of the breach notification provisions.” HHS states that in most cases, a single notice should be able to satisfy both a state's and HHS's notification requirements.

## Further Information

HHS information on the Breach Notification Rule is available at:  
**<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html>** and **<http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>**.

\*\*\*\*\*