

Hall, Render, Killian, Heath & Lyman is a full service health law firm with offices in Indiana, Kentucky, Michigan and Wisconsin. Since the firm was founded by William S. Hall in 1967, Hall Render has focused its practice primarily in the area of health law and is now recognized as one of the nation's preeminent health law firms serving clients in multiple states. For more information about the firm please visit us at [www.hallrender.com](http://www.hallrender.com).

Office Locations  
Indiana Offices  
One American Square  
Suite 2000  
Indianapolis, IN 46282  
(317) 633-4884

8402 Harcourt Road  
Suite 820  
Indianapolis, IN 46260  
(317) 871-6222

Kentucky Office  
614 West Main Street  
Suite 4000  
Louisville, KY 40202  
(502) 568-1890

Michigan Offices  
Columbia Center, Suite 315  
201 West Big Beaver Road  
Troy, MI 48084  
(248) 740-7505

2369 Woodlake Drive, Suite  
280  
Okemos, MI 48864  
(517) 703-0921

Wisconsin Office  
111 East Kilbourn Avenue  
Suite 1300  
Milwaukee, WI 53202  
(414) 721-0442

Contact Us  
[hallrender@hallrender.com](mailto:hallrender@hallrender.com)

## NEW HIPAA BREACH NOTIFICATION RULE

On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (the "Recovery Act"). Title XIII of the Recovery Act is known as the Health Information Technology for Economic and Clinical Health Act ("HITECH"). Among other provisions, HITECH makes several changes to the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Due to the significance of those changes, we will be issuing a series of articles providing an analysis of each of those changes in detail. This is the second in a series of seven such articles.

Previously, HIPAA did not require covered entities to notify individuals or the Department of Health and Human Services ("HHS") when their Protected Health Information ("PHI") was improperly disclosed, although notification was sometimes part of a covered entity's effort to mitigate harm to an individual caused by a wrongful disclosure. HITECH significantly changes HIPAA in this regard because it will require notification of certain breaches to unsecured PHI. The effective date for compliance is expected to be September 17, 2009, which gives covered entities, business associates, and other organizations subject to this new rule only a few months to get ready to comply.

### ***Effective Date.***

The expected effective date for compliance is September 17, 2009, but it depends upon when HHS issues regulations on this new rule. The actual effective date for compliance will be 30 days after the regulations are issued. The statute requires HHS to issue regulations within 180 days after the enactment of HITECH, commonly calculated to be August 17, 2009.

### **New Breach Notification Rule**

How the new rule applies will depend on the type of entity involved. Under the new rule, covered entities will be required to notify individuals of unsecured PHI that has been, or is reasonably believed to have been, accessed, acquired or disclosed due to a breach. Business associates will be required to notify the covered entity of such breaches.

Vendors of personal health records ("PHR") will be required to notify individuals and the Federal Trade Commission ("FTC") of breaches to unsecured individually identifiable information in a PHR. Third party service providers who provide services to a PHR vendor will be required to notify the vendor of such a breach.

## ***Unsecured PHI***

HITECH defines the term “unsecured PHI” as PHI “that is not secured by a technology or methodology specified by” HHS through guidance. HITECH requires HHS to issue such guidance within 60 days of enactment (calculated to be April 17, 2009) and annually thereafter. As of the date of this article, April 13, 2009, HHS has not issued such guidance. Until such guidance is issued, HITECH directs the industry to rely on the technology standards endorsed by the American National Standards Institute (“ANSI”). Under the ANSI standards, PHI that is rendered unusable, unreadable or indecipherable will be considered secured. All other PHI will be considered unsecured, and breach of such PHI will be subject to the breach notification rule.

## ***Breach Notification Methods for Covered Entities***

The methods for breach notification depend in part on the size of the group of individuals affected. Accordingly, covered entities must utilize the following methods:

- First class mail to individuals (or email if preferred by individuals).
- If contact information for 10 or more individuals is out of date, notice must also be posted on the covered entity’s website or notice must be published in “major print or broadcast media.”
- If more than 500 residents of a state are affected, notice must also be published in “prominent media outlets.”
- If 500 or more individuals are affected, immediate notice must also be given to HHS (HHS will post information about the breach on the HHS website).
- An annual log must also be submitted to HHS of all breaches involving less than 500 individuals.

## ***Business Associate Must Notify Covered Entity***

A business associate must notify the covered entity of breaches of unsecured PHI. We note that this breach notification requirement is in addition to the current Privacy and Security Rule requirements, per the business associate agreement, to notify the covered entity of any use or disclosure not permitted by the agreement and of any “security incident.”

## ***Content of Notice***

The notice must contain the following information:

- Description of the incident
- Date of the breach
- Date the breach was discovered
- Description of types of unsecured PHI involved (e.g., name, SSN, DOB, etc.)
- Steps an individual should take to protect themselves against

- potential harm
- Description of investigation, mitigation efforts and prevention of future breaches.
- Contact information.

### ***When to Notify***

All notifications must be given without “unreasonable delay,” but no later than 60 days after discovery. Covered entities may require business associates to give earlier notice. Immediate notice must be given if 500 or more individuals are affected. “Discovery” is when the breach becomes known, or reasonably should have been known. Notification may be put on hold by a law enforcement official if the notification would impede investigation or impact national security.

### ***Breach Notification - Exceptions***

The following instances will not be considered a breach requiring notification:

- An unintentional access of PHI by a covered entity or business associate workforce member, while performing his/her duties, and the information was not further used or disclosed.
- An inadvertent disclosure of PHI by one workforce member to another at the same facility and the PHI was not further used or disclosed.

### ***Still Need to Comply with Other Rules***

Organizations need to keep in mind that even if the new breach notification requirement is not triggered, they still may be required to take the following actions in the case of a breach or other wrongful use or disclosure, when applicable under the current law:

- Mitigate harm for improper use or disclosure
- Log the wrongful disclosure in the accounting
- Impose disciplinary sanctions
- Report security incidents
- Notify individuals under state identify theft law or other similar notification laws.

We note that state law preemption issues are unsettled at this point in time. We expect HHS to address preemption in future rule making. In the meantime, organizations should strive to comply with both federal and state law.

## ***Breach Notification Action Items***

To prepare for the expected effective date of September 17, 2009, organizations should begin to undertake the following steps:

- Adopt new, or revise existing, policies and procedures regarding identifying and responding to breaches.
- Identify which types of PHI are unsecured.
- Evaluate whether unsecured PHI can be made secure through ANSI technologies or methodologies.
- Review e-security for all PHI.
- Create a process for breach response to ensure all breaches are appropriately handled.

If you need additional information about this topic, please contact your regular Hall Render attorney or:

Elizabeth Callahan-Morris at (248) 457-7854 or [ecallahan@hallrender.com](mailto:ecallahan@hallrender.com)

This information is intended for general information purposes only and does not and is not intended to constitute legal advice. The reader must consult with legal counsel to determine how laws or decisions discussed herein apply to the reader's specific circumstances.