

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  
Contact: Mark J. Swearingen

8402 Harcourt Road  
Suite 820  
Indianapolis, IN 46260  
(317) 871-6222  
Contact: Charise R. Frazier

##### Kentucky Office

614 West Main Street  
Suite 4000  
Louisville, KY 40202  
(502) 568-1890  
Contact: Rene R. Savarise

##### Michigan Offices

Columbia Center, Suite 315  
201 West Big Beaver Road  
Troy, MI 48084  
(248) 740-7505  
Contact: Elizabeth Callahan -  
Morris

2369 Woodlake Drive, Suite 280  
Okemos, MI 48864  
(517) 703-0921  
Contact: Brian F. Bauer

##### Wisconsin Office

111 East Killbourn Avenue  
Suite 1300  
Milwaukee, WI 53202  
(414) 721-0442  
Contact: Monica C. Hocum

#### **Contact Us**

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

## **Stimulus Bill Makes Several Significant Changes To HIPAA**

On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (the "Act"). Among other provisions, the Act makes several significant changes to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Unless otherwise indicated, these changes will become effective on February 17, 2010. Persons affected by these changes will need to be prepared to adopt or amend their policies, and practices to comply with the changes. The changes include the following:

***Broader Application to Business Associates.*** The Act broadens the application of HIPAA to business associates. Specifically, the Act provides that business associates must comply with the administrative, physical and technical safeguards and related documentation requirements specified in the HIPAA Security Rule in the same manner as if it was a covered entity. Additionally, the Act provides that the other security and privacy provisions included in the Act apply to business associates in the same manner that they apply to covered entities, and must be incorporated into business associate agreements. Notably, business associates that violate the security or privacy provisions will be subject to the same civil and criminal penalties as would be imposed on the covered entity.

***New Category of Business Associates.*** An organization that transmits protected health information ("PHI") to a covered entity and that routinely requires access to such PHI will be treated as a business associate of the covered entity. Examples of such entities include Health Information Exchange Organizations, Regional Health Information Organizations, E-Prescribing Gateways, and vendors that contract with a covered entity to allow that covered entity to offer a personal health record ("PHR") to its patients.

***Breach Notification for Covered Entities.*** The Act requires covered entities to notify individuals of privacy or security breaches. Covered entities will now be required to notify individuals of a breach of *unsecured* PHI that compromises the security or privacy of the information. Notice is not required for unintentional access by business associates or members of a covered entity's workforce if the individual obtains the PHI while performing his/her duties and does not further use or disclose the information.

For purposes of this breach notification requirement, PHI is "unsecured" if it is not protected by a technology or methodology specified in guidance

from the Secretary of the Department of Health and Human Services (the "Secretary"). If the Secretary does not issue such guidance by April 18, 2009, information will be considered unsecured if it is not: (i) secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals; and (ii) that is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

If notice is required, in most cases the covered entity will be required to make the notification without unreasonable delay, but in no case later than sixty (60) calendar days of the date the breach is known or should reasonably have been known by the covered entity or a business associate. The Act specifies the required content of any such notice, and provides that the notice should be made in writing and sent by first-class mail to the last known address of the individual (or to the individual's next of kin if the individual is deceased) or, if preferred by the individual, by electronic mail. If in any given situation there are ten (10) or more individuals with out-of-date information that prevents direct written communication, the covered entity must conspicuously post the notice on its Website or disseminate it via print or broadcast media.

Covered entities are required to make an annual report of all breaches of unsecured PHI to the Secretary. If a breach of unsecured PHI involves, or is reasonably believed to involve, PHI regarding more than five hundred (500) individuals (a "Significant Breach"), notice must be provided to the Secretary immediately and must also be reported to prominent media outlets. The Secretary is required to maintain a list of each covered entity that is involved in a Significant Breach and to post the list on the Department of Health and Human Services ("HHS") website. Each year the Secretary must file a report detailing Significant Breaches and the actions taken in response to such breaches with Committees for both the Senate and the House of Representatives.

***Breach Notification for PHR Vendors and Other Non-Covered Entities.*** PHR vendors, entities that access information in a PHR or send information to a PHR, and entities that offer products or services through the websites of PHR vendors or covered entities that offer a PHR (collectively, "PHR Entities") will now be subject to a security breach notification requirement. In the event that *unsecured* identifiable health information is acquired without an individual's authorization, PHR Entities must notify any United States citizen or resident whose information was acquired by an unauthorized person as a result of the breach, as well as the Federal Trade Commission ("FTC"). A third-party service provider that provides services to a PHR Entity must notify the PHR Entity in the event the service provider discovers such a breach.

For purposes of this breach notification requirement, identifiable health information is considered unsecured based on the same standards set forth for unsecured PHI. The FTC is required to issue interim final regulations to carry out these requirements by August 17, 2009. These requirements

will apply to breaches which occur thirty (30) days after the FTC issues such interim final regulations.

***Improved Enforcement.*** The Act contains several provisions designed to improve the enforcement of HIPAA:

- ***Revised and Increased Civil Monetary Penalties.*** Civil violations of HIPAA will now be subject to a broader and more severe range of penalties. HIPAA currently provides for civil monetary penalties of \$100 per violation, with a cap of \$25,000 for all violations of an identical requirement or prohibition during a calendar year. HIPAA also currently provides that no civil monetary penalties may be imposed if: (i) the person did not know (and by exercising reasonable diligence would not have known) that such person committed a violation; or (ii) the failure to comply was due to reasonable cause and not willful neglect, and the failure is corrected within thirty (30) days of the date the person knows (or should have known) that the violation occurred.

The Act eliminated those exceptions and established a set of tiered penalties, as follows: (i) \$100 per violation, with an annual cap of \$25,000, for violations where the person did not know (and by exercising reasonable diligence would not have known) that such person committed a violation; (ii) \$1,000 per violation, with an annual cap of \$100,000, for violations due to reasonable cause and not to willful neglect; (iii) \$10,000 per violation, with an annual cap of \$250,000, for violations due to willful neglect that are corrected within thirty (30) days of the date the person knows (or should have known) that the violation occurred; and (iv) \$50,000 per violation, with an annual cap of \$1,500,000 for violations due to willful neglect that are not corrected within the thirty (30) day period. The \$50,000 per violation/\$1,500,000 per year penalties are the maximum penalty that may be imposed under any of the categories of violations. The Act is careful to point out that the Secretary still has the discretion to use corrective action without a penalty in cases where the person did not know (and by exercising reasonable diligence would not have known) that such person committed a violation.

- ***State Attorney General Enforcement.*** The Act authorizes State Attorneys General to bring civil actions in federal district courts against individuals who violate HIPAA. The State Attorneys General will have the authority to enjoin further violations and to seek damages of up to \$100 per violation, with an annual cap of \$25,000 for all violations of the same standard.
- ***Sharing of Penalties with Persons Harmed.*** Within three (3) years of the enactment of the Act, the Secretary is required to issue a regulation establishing a methodology under which an individual who is harmed by a HIPAA violation may receive a portion of any

civil monetary penalty or monetary settlement collected as a result of that violation.

- *Mandatory Investigations and Penalties for Willful Neglect.* If a preliminary investigation of the facts in a complaint indicates a possible HIPAA violation due to willful neglect, the Act requires the Secretary to investigate the complaint and to impose civil monetary penalties for violations due to willful neglect. The Secretary is required to issue regulations regarding this process by August 17, 2010, and these provisions will go into effect on February 17, 2011.
- *Civil Enforcement of Criminal Matters.* HIPAA currently provides for the Secretary to refer potential criminal violations of HIPAA to the United States Department of Justice ("DOJ") for prosecution. Under the Act, if the DOJ has not prosecuted an individual for alleged criminal violations of HIPAA, the HHS Office for Civil Rights ("OCR") may investigate and impose civil monetary penalties against that individual.

***Application of Criminal Penalties.*** The Act amends the criminal penalty provisions of HIPAA to clarify that criminal penalties for wrongful disclosure of PHI apply to both covered entities and to employees and other individuals who obtain or disclose PHI maintained by a covered entity without authorization.

***Limitation on Minimum Necessary Standard.*** The Act limits a covered entity's discretion for determining what constitutes the minimum necessary amount of information that may be used or disclosed for a specific purpose. Initially, where practicable, covered entities will be required to limit such information to a limited data set. The Act requires the Secretary to issue guidance on what constitutes minimum necessary for purposes of the HIPAA Privacy Rule no later than August 17, 2010.

***Accounting for Disclosures from an Electronic Health Record.*** Covered entities that use an electronic health record ("EHR") must, upon request, provide individuals with an accounting of disclosures of PHI from the EHR for purposes of treatment, payment and health care operations which occurred within the three (3) years prior to the date of the request. This effective date of this requirement is January 1, 2014 for disclosures made by covered entities that currently use EHRs, and the later of January 1, 2011, or the date the EHR is acquired, for all other covered entities. The Secretary may delay these dates by up to two (2) years, if necessary. The Secretary must adopt regulations regarding the content of the accounting that take into consideration both the individual's interest in knowing how PHI is used and disclosed and the administrative burdens to covered entities in providing the accounting.

***Access to Copies in Electronic Format.*** The Act provides individuals with a right to request copies of PHI in an electronic format if the covered

entity maintains an EHR, and limits the cost of obtaining the copy to the labor cost related to preparing the response.

***Prohibition On the Sale of Electronic Health Records or PHI.*** PHI cannot be sold unless the covered entity or business associate obtains an authorization from the individual including a statement regarding whether the PHI can be further exchange or sold by the entity that receives the information. The prohibition does not apply if the purpose of the exchange is for:

- public health activities;
- research purposes (if the price charged reflects the cost of preparation and transmittal of the information);
- treatment of the individual;
- health care operations related to the sale, merger or consolidation of a covered entity;
- performance of services by a business associate on behalf of a covered entity;
- providing the individual with a copy of the PHI maintained about him/her; or
- other reasons determined necessary and appropriate by the Secretary.

The Secretary is required to adopt regulations to facilitate this provision no later than August 17, 2010.

***Contacts with Individuals Related to Marketing and Fundraising.*** The Act clarifies that communications by a covered entity or a business associate to individuals about a product or service that encourages the purchase of said product or service does not fit within the definition of health care operations, unless the communication regards a health-related product or service. Instead, such communications generally will be considered marketing under HIPAA and subject to an authorization requirement.

The Act also modified the fundraising provisions of HIPAA to require that each fundraising communication include a conspicuous statement that the individual can "opt out" of future fundraising communications.

***Education on Health Information Privacy.*** No later than August 17, 2009, the Secretary must designate an individual in each regional HHS office to provide guidance to covered entities, business associates, and individuals about their respective rights and responsibilities with regard to the privacy and security of PHI. By February 17, 2010, the OCR must develop a national program to educate individuals about how their PHI is used, the effects of such use, and their rights relative to PHI maintained about them.

***Restriction of Disclosures to Health Plans.*** The Act allows individuals to restrict disclosure of PHI to health plans for purposes of payment or health

care operations if the individual pays the entire cost of the health care service or item.

**Audits.** The Act requires the Secretary to periodically audit covered entities and business associates for compliance with HIPAA.

**Annual Reports.** The Act requires several studies and reports to determine the impact of the Act on HIPAA compliance, including: (i) annual reports by the Secretary regarding a variety of topics, including the number of complaints under HIPAA, how those complaints were resolved (including penalties), and the number of compliance reviews and audits conducted; (ii) a report by the Secretary, in consultation with the FTC, on the application of the Act to entities that prior to the Act were not covered entities or business associates; (iii) guidance by the Secretary regarding how best to implement the requirements for de-identification of PHI; (iv) a report by the U.S. Government Accountability Office ("GAO") on the best practices related to the disclosure of PHI among health care providers for purposes of treatment; (v) a report by GAO no later than February 17, 2014, regarding the impact of the Act on health insurance premiums, overall health care costs, adoption of electronic health records by providers, and reduction in medical errors and other quality improvements; and (vi) a study by the Secretary regarding the definition of "psychotherapy notes."



These changes to HIPAA are significant and will require focused attention and effort in order to meet the deadlines for compliance. Entities affected by these changes should start planning to make the necessary adjustments as soon as possible so that they will be in full compliance by those deadlines.

Should you have any questions or concerns regarding this Alert, please contact Mark J. Swearingen at (317)-977-1458 or [mswearingen@hallrender.com](mailto:mswearingen@hallrender.com) or Monica C. Hocum at (414)-721-0454 or [mhocum@hallrender.com](mailto:mhocum@hallrender.com).

This publication 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.