



ALERT

Stimulus Bill Expands HIPAA Privacy and Security Requirements

. . .

In addition to the massive spending provisions of the American Recovery and Reinvestment Act of 2009 (the “ARRA” or the “Stimulus Bill”) the bill significantly expands the applicability of the Privacy and Security Rules of the Health Insurance Portability and Accountability Act (HIPAA). These changes are likely to have a profound impact throughout the healthcare industry. Title XIII of the ARRA, entitled “Health Information Technology,” also known as the “Health Information Technology for Economic and Clinical Health Act (HITECH Act),” purports to rectify certain perceived weaknesses within the privacy and security regime created by HIPAA. While there are a number of provisions with different effective dates, covered entities and business associates must comply with most of the new provisions discussed below by February 10, 2010.

Business Associates Are Directly Subject to Privacy & Security Rules

New provisions which directly subject business associates to the HIPAA Privacy and Security Rules are intended to close what was perceived by regulatory authorities and certain privacy groups as significant gaps in the scope of HIPAA. HIPAA currently applies only to covered entities (healthcare providers, health plans, healthcare clearinghouses, etc.), and not to third-party service providers. These service providers, referred to as business associates, are indirectly regulated through business associate agreements that they enter into with covered entities. The ARRA imposes HIPAA’s requirements to have and maintain written policies and procedures and to implement administrative, physical and technical information safeguards directly upon business associates “in the same manner that such sections apply to the covered entity.” It also subjects business associates to civil and criminal penalties for violations, which could be up to 10 years in prison and \$250,000 for improper use of Protected Health Information (“PHI”). The Secretary of The Department of Health and Human Services (“HHS”) will publish annual guidance regarding “the most effective and appropriate technical safeguards” for this purpose.

Furthermore, a business associate that obtains or creates PHI pursuant to a written contract or arrangement may only use or disclose PHI in compliance with each applicable requirement of 45 C.F.R. §164.504(e), which sets forth the detailed requirements for implementation of a business associate agreement. Effectively, this means that regardless of the provisions of the business associate

ALERT

agreement between the business associate and the covered entity, business associates will be directly responsible for full compliance with the relevant requirements of the privacy rule itself. The bill also adds an additional burden for a business associate to take action when it knows of a pattern or practice of activity on the part of the covered entity in violation of the privacy standard. Accordingly, a business associate violates the privacy rule and is subject to civil and criminal penalties, if it knows of violations by the covered entity and takes no action. This provision has the potential to cause tension and litigation between business associates and covered entities.

New Data Breach Notification Requirements

Effective 30 days after HHS publishes implementing interim final regulations, covered entities must notify each individual affected by a breach of “unsecured” PHI and maintain a log of such breaches to be submitted to HHS on an annual basis. “Unsecured” PHI is essentially PHI that is not encrypted. HHS is required to publish these regulations by August of 2009. This notification requirement is generally consistent with many state law notification provisions, but is more stringent in the following ways. First, the breach is deemed to be discovered on the first day that the breach is known or should reasonably have been known by the entity (which includes any employee, officer or agent other than the individual committing the breach). Second, the individual notification must be provided to the consumer within 60 days of discovery. Furthermore, if a breach involves 500 or more individuals, a covered entity must also notify major media outlets and HHS immediately. Business associates must report a data security breach to covered entities within the same timeframes or be subject to direct enforcement and penalties.

Temporary “Minimum Necessary” PHI Standard

HIPAA currently requires covered entities to use, disclose and request only the “minimum necessary” amount of PHI for non-treatment purposes. Under the ARRA, in order to satisfy the minimum necessary requirements, a covered entity must now limit its requests for, uses or disclosures of PHI to a Limited Data Set, “to the extent practicable.” A Limited Data Set is still considered PHI under HIPAA, but the data has been stripped of all direct identifiers. The Secretary of HHS must issue guidance as to what constitutes “minimum necessary” within 18 months of the ARRA’s enactment, at which time this provision will sunset.

Same Security Breach Notification Requirements for PHR Vendors & Service Providers

A PHR is defined as “an electronic record of PHR identifiable health information... on an individual that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual.” A “Vendor of Personal Health Records” is defined as “an entity, other than a covered entity...that offers or maintains a personal health record.” The ARRA imposes upon PHR vendors the same obligations as covered entities with respect to data security breaches and the same obligations of business associates upon third party service providers of PHR vendors. PHR vendors are required initially to report breaches to the Federal Trade Commission (“FTC”) which will then notify HHS. A PHR vendor’s failure to comply with these requirements will be considered an “unfair and deceptive trade practice” within the jurisdiction of the FTC. It should be noted, however, that these provisions of the ARRA are temporary provisions. They will have the same effective date as the analogous provisions for covered entities and business associates, but they will sunset if Congress enacts legislation establishing requirements for security breach notifications applicable to entities that are neither covered entities nor business associates.

Boston

One Financial Center
Boston, MA 02111
+1.617.856.8200
+1.617.856.8201 [fax]

Hartford

City Place I
185 Asylum Street
Hartford, CT 06103
+1.860.509.6500
+1.860.509.6501 [fax]

New York

Seven Times Square
New York, NY 10036
+1.212.209.4800
+1.212.209.4801 [fax]

Providence

121 South Main Street
Providence, RI 02903
+1.401.276.2600
+1.401.276.2601 [fax]

Washington, DC

601 Thirteenth Street NW,
Suite 600
Washington, DC 20005
+1.202.347.2222
+1.202.347.4242 [fax]

London

8 Clifford Street
London, W1S 2LQ
United Kingdom
+44.20.7851.6000
+44.20.7851.6100 [fax]

Dublin

Alexandra House
The Sweepstakes
Ballsbridge, Dublin 4
Ireland
+353.1.664.1738
+353.1.664.1838 [fax]

www.brownrudnick.com

Information contained in this Alert is not intended to constitute legal advice by the author or the attorneys at Brown Rudnick LLP, and they expressly disclaim any such interpretation by any party. Specific legal advice depends on the facts of each situation and may vary from situation to situation.

Distribution of this Alert to interested parties does not establish an attorney-client relationship. The views expressed herein are solely the views of the authors and do not represent the views of Brown Rudnick LLP, those parties represented by the authors, or those parties represented by Brown Rudnick LLP.

Increased Consumer Rights

Under the new provisions of the ARRA, if requested by a consumer, a covered entity is prohibited from disclosing PHI for payment or healthcare operations if the information pertains to a healthcare item or service that the consumer paid for in full out of pocket. The one exception is when the disclosure is otherwise required by law or required for treatment purposes. This provision allows consumers to prevent certain information from being available to their insurers for treatments that would affect their rates or insurability.

In addition, covered entities that utilize electronic health records must, upon the consumer's request, provide the consumer with a copy of his or her information in electronic format, and, if so directed by the consumer, must also transmit the copy directly to a recipient designated by the consumer. This provision is intended to simplify the ability of consumers to have their information flow from their healthcare providers into their PHR.

Until the February 17, 2010 effective date of most of these provisions, it is expected that HHS will clarify how these new provisions will be applied and interpreted. In the interim, it would be prudent for covered entities and business associates to evaluate, and amend as necessary, all of their existing business associate agreements in order to ensure compliance. Business associates should also evaluate their internal protocols and procedures for safeguarding PHI.

Brown Rudnick is an international law firm with offices in the United States and Europe. Our 200 attorneys provide assistance across key areas of the law, including employment law, complex litigation and arbitration, bankruptcy and finance, corporate and securities, intellectual property, real estate, energy, and government law and strategies.

If you have any questions about how these new provisions will impact your organization, or would like assistance in reviewing your existing agreements or policies, please contact one of the following Brown Rudnick attorneys:

Robert J. Anthony
+1.860.509.6517
ranthony@brownrudnick.com

James L. Hauser
+1.617.856.8130
jhauser@brownrudnick.com

Rebecca F. Alperin
+1.617.856.8318
ralperin@brownrudnick.com

Marc C. Lombardi
+1.860.509.6510
mlombardi@brownrudnick.com

