

Health Care ADVISORY

June 26, 2009

The HITECH Act: Business Associates Now Directly Covered by HIPAA

Overview

The recent economic stimulus legislation, the American Recovery and Reinvestment Act (ARRA),¹ has been the subject of much political debate. Although overlooked by many of the media and political commentators, ARRA contained a section called the Health Information Technology for Economic and Clinical Health Act (“HITECH Act” or “Act”). The HITECH Act greatly impacts the health care industry and makes sweeping changes to the HIPAA Privacy and Security Rules (the “HIPAA Rules”). Most significantly, the HITECH Act for the first time makes the HIPAA Rules, as well as the civil and criminal penalties under the HIPAA Statute, applicable to business associates (BAs)—i.e., entities providing services to health care providers, health insurers and other HIPAA “covered entities.”

Before the HITECH Act, the HIPAA Rules applied directly only to covered entities—i.e., health care providers, health plans and health care clearinghouses (“Covered Entities”). Covered Entities were required to have contracts with those service providers whose services to the Covered Entities involved receipt of protected health information (PHI), and those Business Associate Agreements (BAAs) that passed along certain specified privacy protections for the PHI handled by the BAs. None of the enforcement provisions and penalties for HIPAA violations applied directly to BAs, and a breach of a BAA resulted only in contractual remedies.

That was then; this is now. The HITECH Act now has greatly changed how the HIPAA Rules apply to BAs, including enforcement actions and penalties. Every BA should review the HITECH Act carefully and take action to comply with its new responsibilities under the Act and the HIPAA Rules.

What’s New For Business Associates

The HITECH Act expands the application of the HIPAA Rules to BAs, and various effective dates apply for different provisions of the Act. This memo provides an overview of the biggest changes, and BAs should review and revise their BAAs now to account for the key HITECH Act changes, including:

- prohibition on sales of electronic health records (EHR) or PHI;

¹ American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (2009).

- limitation of PHI disclosures to limited data sets;
- applicability of civil and criminal penalties for violations;
- mandatory compliance audits by the Secretary of the Department of Health and Human Services (the “Secretary”); and
- expansion of types of entities that are required to have BA agreements
- new restrictions on marketing communications.

BA Liability for Violation of the HIPAA Privacy and Security Rules

Under the HITECH Act, the HIPAA Privacy and Security rules apply directly to BAs, and HIPAA criminal and civil penalties for violations apply directly to BAs, as well.

Under the HITECH Act, a BA is permitted to use or disclose PHI only in compliance with the sections of the HIPAA Rules defining the obligations of a BA.² In other words, under the HITECH Act, a breach of a BAA now constitutes a violation of law, as well as a breach of contract.

BAs will be required to meet a broad range of requirements previously applicable only to Covered Entities under the HIPAA Rules, such as obtaining patient authorization for certain uses and disclosures of PHI, establishing privacy and security policies and procedures, providing patients with rights of access, amendment and an accounting of disclosures, conducting a security risk assessment for electronic PHI and many of the other extensive requirements of the HIPAA Rules.

Additionally, under the HITECH Act, a BA is subject to sanctions if it has knowledge of a pattern or practice that would constitute a material breach or violation of its BAA with a Covered Entity, and subsequently fails to take action to cure the breach or terminate the agreement.³ The effect of this provision appears to be that a BA violates the law if it learns that a Covered Entity to which it provides services commits a material breach under its BAA and it fails to take action to cure the breach or terminate the contract.

The HIPAA Security Rules relating to administrative, physical and technical safeguards of electronic PHI (plus the new security requirements under the HITECH Act that apply to Covered Entities) will apply directly to BAs in the same way that those standards apply to Covered Entities.⁴ Significantly, the civil and criminal penalties that apply for violating these security standards now will apply directly to BAs.⁵

² HITECH Act at § 13404(a).

³ HITECH Act at § 13404(b); *see also* 45 C.F.R. § 164.504(e)(1)(ii).

⁴ HITECH Act at § 13401(a).

⁵ HITECH Act at § 13401(b).

The effective date of these provisions subjecting BAs to privacy and security requirements under the HITECH Act is February 17, 2010. The full effects of these changes on BAs will not be clear until the Secretary issues implementing regulations.

Notification Requirements For BAs In Case Of a Security Breach

The HITECH Act creates a new notice requirement for BAs for security breaches involving PHI. The Act requires a BA that discovers a security breach of “unsecured PHI” to notify the Covered Entity not later than 60 calendar days after discovery of the breach, unless the notification would impede a criminal investigation or harm national security.⁶ Significantly, the HITECH Act provides that a breach is “discovered” (1) on the first day on which the breach is known to a person other than the person committing the breach who is an employee, officer or other agent of the entity; or (2) on the first day that such a person reasonably should have known of the breach.⁷

In implementing this security breach notification requirement, the Secretary is instructed to issue interim final regulations within 180 days of enactment of the HITECH Act, meaning that those regulations should be issued by August of this year. The notification requirements will be effective for breaches discovered on or after 30 days from when the interim final regulations are published. In connection with the forthcoming breach notification requirements, the Secretary issued guidance (the “Guidance”) on April 17, 2009, regarding the acceptable methods of securing PHI—including standards for encryption and disposal of PHI.⁸ BAs should take steps now to comply with the Guidance so that they will be safe harbored from the breach notification requirements when the compliance date arrives in September.

Because of the short timeframe in which BAs must comply with these new requirements, BAs should begin now to implement the specified security measures and technologies to safeguard PHI, and should revise their BAAs to reflect those new security measures.

Additional Restrictions on Certain Disclosures by BAs

Under the HITECH Act, individuals will have the right to receive an accounting of PHI disclosures made by Covered Entities for treatment, payment and health care operations during the previous three years if the Covered Entity uses or maintains an EHR with respect to PHI.⁹ Specifically, a Covered Entity is required to provide either (1) an accounting of disclosures by the Covered Entity and by a BA acting on the Covered Entity’s behalf or (2) an accounting of disclosures made by the Covered Entity and a list of all the BAs acting on behalf of the Covered Entity, including their contact

⁶ HITECH Act at § 13402.

⁷ HITECH Act at § 13402(c).

⁸ 74 *Fed. Reg.* 19006 (April 27, 2009). Under Section 13402(h)(2) of the Act, the Secretary was required (in consultation with stakeholders) to issue guidance that specifies the technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals (i.e., encryption).

⁹ HITECH Act at § 13405(c).

information. For the latter alternative, if a BA is included on the list, the BA must provide an accounting of disclosures in response to an individual's direct request to the BA.

Accordingly, BAs will be required not only to maintain a record of the required disclosures, but also to implement a procedure for responding to patient requests. It is important to note that this BA requirement will apply when a Covered Entity uses an EHR and chooses to list the BA in responding to the patient request. And the requirement will apply to the BA, even if the BA does not use or maintain an EHR itself.

The Secretary must issue regulations on the information to be included in these disclosures not later than six months after the Secretary adopts the applicable standards. For Covered Entities that already use EHRs, the accounting requirement will apply for disclosures made on or after January 1, 2014. For Covered Entities that do not currently use EHRs, the accounting requirement will apply for disclosures made on the later of January 1, 2011, or when the Covered Entity acquires EHRs. The Secretary also may impose a subsequent effective date of not later than 2016 for current EHR users and of not later than 2013 for non-users of EHRs.

Limiting Disclosures to Limited Data Sets

The HITECH Act requires the Secretary to issue guidance by August 16, 2009, on what constitutes the "minimum necessary" amount of PHI to accomplish the intended purpose of a use or disclosure of PHI. Until this guidance is issued, BAs should limit the use, disclosure or request for PHI, to the extent practicable, to a limited data set¹⁰ or, if more information is needed, to the minimum necessary amount of PHI to accomplish the intended purpose of the use, disclosure or request.¹¹ For purposes of this requirement, BAs are tasked with determining what constitutes the minimum necessary amount of PHI to accomplish the intended purpose of the disclosures of PHI that it makes in providing services to the Covered Entity. BAs should review the types of disclosures they make on a routine basis and confirm that the information disclosed constitutes a limited data set or that the disclosures are limited to the minimum necessary amount of PHI to accomplish the intended purpose of the disclosure.

Prohibition on Sales of Electronic Health Records (EHR) or PHI

The HITECH Act has toughened the prohibition on selling PHI by specifically prohibiting a Covered Entity or BA from receiving remuneration in exchange for PHI without an individual's authorization, unless the exchange is made for certain enumerated purposes.¹² These purposes include the following: (1) public health activities; (2) research, if the price charged reflects the costs of preparation and transmittal of data; (3) treatment of the individual; (4) the sale, transfer, merger or consolidation of all or part of a Covered Entity with another Covered Entity, and due diligence related to that activity;

¹⁰ Under the HIPAA Rules, the term "limited data set" refers to PHI from which certain specified direct identifiers of individuals and their relatives, household members and employers have been removed. See 45 C.F.R. § 164.514(e).

¹¹ HITECH Act at § 13405(b).

¹² HITECH Act at § 13405(d).

(5) paying a BA under a BAA for services rendered; (6) providing an individual with access to his or her PHI; or (7) an exchange made pursuant to an arrangement determined by the Secretary to be similarly necessary and appropriate as the enumerated exceptions. The Secretary is instructed to issue regulations related to this prohibition by August 16, 2009. BAs should now review their BAAs to ensure that, if payment is made between a Covered Entity and the BA, those payment terms are contained in the BAA and no other remuneration is received by the BA in exchange for the PHI, unless one of the other above-listed exceptions applies.

BAs Face Civil Penalties and Criminal Liability for Violations (Ouch!)

The HITECH Act fundamentally changes the enforcement of HIPAA violations and extends these penalties and liabilities to BAs.¹³

- First, the HITECH Act amends the HIPAA Statute to permit the Office of Civil Rights (OCR) to pursue an investigation and the imposition of civil monetary penalties (CMPs) against any individual (not just the Covered Entity or BA) for an alleged criminal violation of the HIPAA Rules, if the Justice Department has not prosecuted the individual. That is, even if the violation constitutes a criminal offense, OCR can impose CMPs, as long as the individual has not been prosecuted criminally. The Secretary must issue regulations by August 16, 2009, which will apply to penalties imposed on or after February 16, 2011.
- Second, the HITECH Act will *require* a formal investigation and imposition of CMPs for violations due to willful neglect. To carry out this change, the Secretary must issue regulations by August 16, 2009, that will apply to penalties imposed on or after February 16, 2011. Thus, it appears the Secretary currently *may* impose the new CMPs now for violations involving willful neglect (based on the effective dates discussed below). However, once the willful neglect provisions are effective, the Secretary will be *required* to impose CMPs for those violations.
- Third, the HITECH Act authorizes any state attorney general to bring a civil action in federal district court against individuals who violate the HIPAA Rules. The state attorney general now will have this right of action either to enjoin violations or to seek damages of up to \$100 for each violation, and \$25,000 for all similar violations within a calendar year. These provisions are effective after February 17, 2009.
- Fourth, the HITECH Act establishes four new tiers of CMPs. The CMPs would range from \$100 to \$50,000 for each violation, and from \$25,000 to \$1,500,000 for similar violations within a calendar year. The tiers of CMPs are based on the level of culpability, covering the spectrum from no knowledge of the violation to willful neglect. These provisions are effective for violations occurring after February 17, 2009.

¹³ HITECH Act at § 13410.

- Lastly, the Government Accountability Office (GAO) is charged with recommending to the Secretary a methodology under which harmed individuals under HIPAA would receive a percentage of any CMP or monetary settlement collected with respect to a HIPAA violation. Based on GAO's recommendations, the Secretary must establish regulations for implementing this methodology by February 16, 2012.

Mandatory Compliance Audits by the Secretary

BAs should prepare now for mandatory compliance audits. The HITECH Act requires the Secretary to conduct periodic audits of BAs to ensure their compliance with the HIPAA Rules, as amended by the HITECH Act and its implementing regulations.¹⁴ This requirement is effective as of February 17, 2010. Thus, in preparation for that date, BAs should take action to make sure they are in compliance with the applicable security and privacy requirements and that they have documentation (e.g., policies and procedures) demonstrating their compliance.

More Entities Must Have BA Agreements

The HITECH Act has expanded the types of entities required to enter into BAAs with Covered Entities. The Act requires that certain organizations that provide data transmission of PHI to a Covered Entity (or its BA) and that require access on a routine basis to such PHI be treated as BAs; therefore, those organizations must have a BA agreement with the Covered Entity.¹⁵ In effect, certain entities treated as "trading partners" under the HIPAA Transaction Standards Regulations¹⁶ now must establish a BA agreement with the Covered Entity. Specifically, affected entities include a Health Information Exchange Organization, a Regional Health Information Organization (RHIO), an E-prescribing Gateway and each vendor that contracts with a Covered Entity to allow that Covered Entity to offer a personal health record (PHR) to patients as part of its EHR system.¹⁷ These provisions will be effective February 17, 2010.

Additional Restrictions on BA Marketing Communications

The HITECH Act also addresses marketing communications made by BAs. The HITECH ACT clarifies that a marketing communication by a BA about a product or service that encourages the recipient to purchase or use the product or service may not be considered an otherwise permissible "health care operation," unless the communication relates to a health care-related product or service offered by the Covered Entity, or the communication otherwise relates to the treatment of the individual.¹⁸ These marketing provisions will be effective on February 17, 2010. BAs should

¹⁴ HITECH Act at § 13411.

¹⁵ HITECH Act at § 13408.

¹⁶ See 45 C.F.R. §§ 160.103 and 162.915.

¹⁷ A PHR is an individually identifiable electronic record of PHI that is maintained by, or on behalf of, an individual.

¹⁸ HITECH Act at § 13406(a).

review whether their communications to patients constitute marketing and, if so, should limit those communications so they relate to a Covered Entity-offered health care product or service or relate to the individual's treatment.

Conclusion

The HITECH Act is a serious matter for BAs. The HITECH Act has significantly changed how the HIPAA Rules apply to BAs and how the HIPAA Rules can be enforced against BAs. Instead of being subject only to contractual obligations for handling PHI, BAs now are covered directly by the extensive requirements of the HITECH Act and the HIPAA Rules, and significant civil and criminal penalties can be imposed against BAs for failing to comply with them.

Each BA should act now to review: (1) the information security measures it employs to protect PHI, (2) its policies and procedures relating to PHI it handles for Covered Entity clients, (3) its BA agreements, (4) the ways in which it uses and discloses PHI and the amount of PHI disclosed and (5) its communications to patients, if any, to implement measures to meet these new requirements. Also, BAs should prepare for the compliance audits that will be coming by implementing appropriate written policies and maintaining documentation to demonstrate their compliance with the new privacy and security requirements for PHI as they become effective. And BAs should assign responsibility for monitoring the development and issuance of the many implementing regulations that will be forthcoming.

For assistance with any of these important tasks, contact an attorney in Alston & Bird's Health Care Group.

If you would like to receive future *Health Care Advisories* electronically, please forward your contact information including e-mail address to health_care.advisory@alston.com. Be sure to put “**subscribe**” in the subject line.

For further guidance please contact one of the attorneys or advisors listed below:

Washington Office

Jacqueline C. Baratian
202.756.3484
jacqueline.baratian@alston.com

Jennifer L. Butler
202.756.3326
jennifer.butler@alston.com

Elinor A. Hiller
202.756.3401
elinor.hiller@alston.com

Laura E. Holland
202.239.3980
laura.holland@alston.com

Peter M. Kazon
202.756.3334
peter.kazon@alston.com

Stephanie A. Kennan
Senior Public Policy Advisor
202.756.3159
stephanie.kennan@alston.com

Keavney F. Klein
202.239.3981
keavney.klein@alston.com

Rudy S. Missmar
202.756.3034
rudy.missmar@alston.com

Mark Rayder
Senior Public Policy Advisor
202.756.3562
mark.rayder@alston.com

Colin T. Roskey
202.756.3436
colin.roskey@alston.com

Marc J. Scheineson
202.756.3465
marc.scheineson@alston.com

Thomas A. Scully
202.756.3459
thomas.scully@alston.com

Donald E. Segal
202.756.3449
donald.segal@alston.com

Tamara R. Tenney
202.756.3489
tamara.tenney@alston.com

Julie K. Tibbets
202.756.3444
julie.tibbets@alston.com

Timothy P. Trysla
202.756.3420
tim.trysla@alston.com

Tiffani V. Williams
202.756.3412
tiffani.williams@alston.com

Marilyn Yager
Senior Public Policy Advisor
202.756.3341
marilyn.yager@alston.com

Atlanta Office

Donna P. Bergeson
404.881.7278
donna.bergeson@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Jeffrey K. Hester
404.881.4254
jeff.hester@alston.com

Robert C. Lower
404.881.7455
bob.lower@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

D'Andrea J. Morning
404.881.7538
dandrea.morning@alston.com

Robert D. Stone
404.881.7270
robert.stone@alston.com

Michelle A. Williams
404.881.7594
michelle.williams@alston.com

ATLANTA

One Atlantic Center
1201 West Peachtree Street
Atlanta, GA 30309-3424
404.881.7000

CHARLOTTE

Bank of America Plaza
Suite 4000
101 South Tryon Street
Charlotte, NC 28280-4000
704.444.1000

DALLAS

Chase Tower
Suite 3601
2200 Ross Avenue
Dallas, TX 75201
214.922.3400

LOS ANGELES

333 South Hope Street
16th Floor
Los Angeles, CA 90071-3004
213.576.1000

NEW YORK

90 Park Avenue
New York, NY 10016-1387
212.210.9400

RESEARCH TRIANGLE

Suite 600
3201 Beechleaf Court
Raleigh, NC 27604-1062
919.862.2200

SILICON VALLEY

Two Palo Alto Square
Suite 400
3000 El Camino Real
Palo Alto, CA 94306-2112
650.838.2000

VENTURA COUNTY

Suite 215
2801 Townsgate Road
Westlake Village, CA 91361
805.497.9474

WASHINGTON, D.C.

The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202.756.3300

www.alston.com

© Alston & Bird LLP 2009