



*presents*

# **HITECH's Impact on Business Associate Agreements With Healthcare Providers**

## **Complying With New HIPAA Requirements and Preparing for Tougher Enforcement**

**A Live 90-Minute Teleconference/Webinar with Interactive Q&A**

**Today's panel features:**

Shirley P. Morigan, Partner, **Foley & Lardner**, Los Angeles

Melissa K. Bianchi, Partner, **Hogan & Hartson**, Washington, D.C.

Rachel Nosowsky, Senior Counsel, **Miller Canfield Paddock and Stone**, Ann Arbor, Mich.

**Thursday, February 25, 2010**

The conference begins at:

**1 pm Eastern**

**12 pm Central**

**11 am Mountain**

**10 am Pacific**

You can access the audio portion of the conference on the telephone or by using your computer's speakers.  
Please refer to the dial in/ log in instructions emailed to registrations.

CLICK ON EACH FILE IN THE LEFT HAND COLUMN TO SEE INDIVIDUAL PRESENTATIONS.

If no column is present: click **Bookmarks**  or **Pages**  on the left side of the window.

If no icons are present: Click **View**, select **Navigational Panels**, and chose either **Bookmarks** or **Pages**.

If you need assistance or to register for the audio portion, please call Strafford customer service at **800-926-7926 ext. 10**

**BAA Checklist**  
*by Rachel Nosowsky, Esq.*

*Mandatory Terms*

- Establishes permitted and required uses and disclosures of PHI by the BA [generally may not authorize the BA to use or further disclose the information in a manner that would violate HIPAA if done by the CE] .
- Prohibits BA from using or disclosing PHI other than as permitted or required in the contract or as required by law.
- Requires BA to use appropriate safeguards to prevent use or disclosure of PHI other than as provided in the agreement (and under the security rule to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI the BA creates, receives, maintains, or transmits on behalf of the CE); and to report general violations and security incidents to CE “of which it becomes aware”.
- Requires BA to ensure that agents (including subcontractors) agree to the same restrictions and conditions that apply to the BA.
- Requires BA to make PHI in a designated record set available for access (45 CFR § 164.524) or amendment (45 CFR § 164.526); and to account for unauthorized disclosures (45 CFR § 164.528).
- Requires BA to make internal practices, books, and records relating to the use or disclosure of PHI received from or created or received by the BA on behalf of the CE available to the DHHS Secretary (OCR) for purposes of determining the CE’s compliance with the regulations.
- Requires return or destruction of PHI upon termination (if feasible) or (if not) extension of protections of the contract to any retained information and limitation of further uses or disclosures to purposes that make return/destruction infeasible.
- Authorizes termination of the contract by the CE if the CE determines that the BA has violated a material term of the agreement. In the event of non-compliance with contract terms, requires non-breaching party to take reasonable steps to cure the breach or, if unsuccessful, terminate the contract or report the problem to the DHHS Secretary (OCR).

*Permissive Terms*

- BA may provide data aggregation services relating to the CE’s health care operations
- BA may use PHI for its proper management and administration or to carry out its legal responsibilities; or disclose PHI if required by law or the BA obtains reasonable assurances from the recipient that the information will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed and the recipient agrees to notify the BA of any breaches.
- Create a de-identified or limited data set and further use or disclose consistent with HIPAA requirements (including data use agreement in the case of an LDS).
- Report violations of law.

*Additional Recommended Terms (OCR)*

- Definitions (consistent with HIPAA and, now, HITECH) and regulatory references.
- Mitigation (if appropriate for CE to pass on its duty to mitigate).
- CE obligations: notify BA of applicable NPP limitations, changes in authorization, or agreed-upon restrictions; refrain from requesting BA to do what CE cannot legally do (except for data aggregation and management and administration activities).
- Interpretation, amendment, survival.

*HITECH Considerations*

- Recital of BA's direct regulation under HITECH.
- Application of HIPAA:
  - BA must comply with security rules at 45 CFR §§ 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), 164.316 (policies, procedures, documentation), for example, by appointing a security official and conducting appropriate risk assessments.
  - Direct accounting of disclosures to requesting individuals, if CE furnishes a list of BAs to inquiring individuals.
  - In the event of CE contract violations, BA must seek to cure, terminate the agreement, or report to the DHHS Secretary.
- BA must notify CE of any breach consistent with HITECH requirements.
- Other new HITECH mandates applicable to both parties:
  - Comply with individual requests for restriction of certain disclosures to health plans.
  - Application of minimum necessary standard (and adoption of limited data set safe harbor) ... more guidance TBD by August 2010.
  - Prohibitions on PHI sales (with limited exceptions).
  - Individual right to access EHR information electronically.
  - New restrictions on marketing communications and payment for such communications.
  - New restrictions on fundraising.
- Both parties must be prepared for periodic OCR audits.

*General Considerations*

- Attention to scope (*e.g.*, specify on face of agreement that it applies only if and to the extent the BA is, in fact, a BA to the CE).
- Interpretation and amendment (*e.g.*, to be consistent with HIPAA/HITECH as revised over time).
- Representations and warranties.
- Indemnification and insurance.

*Other (Institution-Specific)*

- State law mandates.
- Red Flag Rules compliance.
- Other: \_\_\_\_\_

**HITECH Implications for Business Associate Agreements:  
What Should You Do and When Should You Do It?**  
*by Rachel Nosowsky, Esq., Miller Canfield Paddock & Stone PLC*

(originally written for ABA *Health eSource*, Vol. 5, No. 10, June 2009)

Title XIII of the American Recovery and Reinvestment Act of 2009 (“ARRA”), called the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, codifies and expands on many of the requirements promulgated by the Department of Health & Human Services (“DHHS”) pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) to protect the privacy and security of protected health information (“PHI”).<sup>1</sup>

For example, HITECH for the first time directly regulates business associates – defined to include persons who, on behalf of a covered entity (but other than as members of the covered entity’s workforce), perform or assist in performing a function or activity that involves the use or disclosure of individually identifiable health information, or that otherwise is regulated by HIPAA.<sup>2</sup> Specifically, effective February 17, 2010, HITECH will:

- Require business associates to comply directly with Security Rule provisions directing implementation of administrative, physical and technical safeguards for electronic protected health information (“e-PHI”); and development and enforcement of related policies, procedures, and documentation standards (including designation of a security official).<sup>3</sup>
- Impose on business associates an obligation to directly comply with HIPAA’s business associate safeguards,<sup>4</sup> including limiting use and disclosure of PHI as specified in the agreement or as required by law; facilitating access, amendment and accounting of disclosures; opening books and records to DHHS; and returning or destroying PHI, if feasible, upon contract termination.<sup>5</sup>
- Deem a business associate to violate HIPAA if the business associate knows of a “pattern of activity or practice” by a covered entity that breaches their business associate agreement (“BAA”), but fails to cure the breach, terminate the BAA, or report the non-compliance to DHHS.<sup>6</sup>
- Require DHHS to conduct compliance audits.<sup>7</sup>

HITECH’s enhanced privacy and security standards are applicable to both covered entities and business associates,<sup>8</sup> and generally also become effective February 17, 2010. They include:

- Breach notification (interim final regulations are due August 17, 2009 and will become effective 30 days later);<sup>9</sup>

---

<sup>1</sup> The security regulations are found at 45 C.F.R. parts 160 and 164, subpart C (“Security Rule”); the privacy regulations are found at 45 C.F.R. parts 160 and 164, subpart E (“Privacy Rule”).

<sup>2</sup> 45 C.F.R. § 160.103; 42 U.S.C. § 17921(2). HITECH makes clear Congress’s intent to regulate certain health information exchanges and personal health record vendors. 42 U.S.C. § 17938.

<sup>3</sup> 42 U.S.C. § 17931(a); 45 C.F.R. §§ 164.308-312; and 164.316.

<sup>4</sup> 42 U.S.C. § 17934(a).

<sup>5</sup> 45 C.F.R. § 164.504(e).

<sup>6</sup> 42 U.S.C. § 17934(b); 45 C.F.R. § 164.504(e)(1)(ii).

<sup>7</sup> 42 U.S.C. § 17940.

<sup>8</sup> 42 U.S.C. §§ 17931, 17934.

<sup>9</sup> 42 U.S.C. § 17932.

- New restrictions on disclosures to health plans, clarified minimum necessary standards, expanded accounting requirements applicable to electronic health records (effective as early as January 2011), and revised prohibitions on sales of PHI;<sup>10</sup>
- Updated marketing and fundraising restrictions;<sup>11</sup> and
- Enhanced civil and criminal penalties for non-compliance.<sup>12</sup>

### *BAA Compliance After HITECH*

Health law practitioners have developed no clear consensus on the implications of HITECH for BAAs, and in particular disagree on whether there is any actual mandate to amend existing agreements. Some argue that because HITECH now directly regulates business associates and directly imposes on them the new privacy and security obligations defined in Subtitle D, it is unnecessary to update existing BAAs. Others point out that Sections 13401 and 13404 explicitly mandate that HITECH's new security and privacy provisions be "incorporated into the business associate agreement[.]"<sup>13</sup>

In truth, the need to amend may well depend on the specific language included in existing BAAs and its interpretation by the parties and, ultimately, DHHS. For example, sample BAA language developed by the Office for Civil Rights provides: "The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and [HIPAA]."<sup>14</sup> While some first-generation BAAs adopted this language wholesale, others provided for automatic amendment or amendment by notice from the covered entity to incorporate any revisions necessary to assure ongoing compliance without the need to re-contract. Some attorneys argue that even the sample language (particularly if previously updated to comply with the Security Rule) adequately addresses any new mandates, as it defines regulatory references to mean those "in effect or as amended" and requires any ambiguity in interpretation of the BAA to be "resolved to permit the Covered Entity to comply" with HIPAA.<sup>15</sup> Given the explicit mandate in HITECH to incorporate its new provisions, the safer approach may well be to amend the agreements, unless DHHS develops a safe harbor to avoid the assumption by covered entities of massive and arguably unnecessary administrative costs. Many covered entities, however, particularly large ones with extensive vendor networks and complex contracting processes, may determine that such costs are prohibitive, notwithstanding the potentially significant penalties the parties could be subject to for failure to adhere to the plain language of the new law.

Additional issues covered entities and business associates should consider in evaluating existing agreements and developing or negotiating new ones include:

1. Who is a Business Associate? Because HITECH imposes direct obligations on business associates and provides for the imposition of civil and criminal penalties on non-compliant business associates, vendors may want to re-evaluate their position. In the past, some vendors who did not believe themselves to be "business associates" as defined in HIPAA willingly signed BAAs because their obligations under those agreements were not, practically speaking, particularly substantial. Others who thought they might be business associates but whose customers failed to ask them to sign BAAs did not press the issue, on the theory that failure to execute a BAA was a compliance problem only for the covered entity. Today, the stakes have changed: a vendor's

---

<sup>10</sup> 42 U.S.C. § 17935.

<sup>11</sup> 42 U.S.C. § 17936.

<sup>12</sup> 42 U.S.C. §§ 17939(a); 17931(b); 17934(c).

<sup>13</sup> 42 U.S.C. §§ 17931(a) and 17934(a).

<sup>14</sup> 67 Fed. Reg. 53182, 53264 (Aug. 14, 2002); *see also* <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html> (accessed May 30, 2009).

<sup>15</sup> *Id.*

acknowledgement that it is a business associate when it is not can unnecessarily expose the vendor to substantial civil and criminal penalties under 42 U.S.C. §§ 1320d-5 and 1320d-6; yet its failure to enter a BAA when one is required would violate HITECH.<sup>16</sup> One way to resolve this conundrum is to provide in a scope statement that the BAA applies only if and to the extent the vendor is a business associate to the covered entity (as defined in HIPAA), and that the vendor does not, by signing the BAA, concede it is one.

2. Security Guidance. HITECH requires DHHS to issue annual guidance on “the most effective and appropriate technical safeguards” to facilitate compliance with the Security Rule.<sup>17</sup> Moreover, the law’s breach notification provisions will apply only to breaches of “unsecured” PHI.<sup>18</sup> PHI is deemed unsecured unless rendered “unusable, unreadable, or indecipherable” to unauthorized individuals by technologies or methodologies explicitly identified in separate guidance issued by DHHS (and currently limited to encryption or destruction<sup>19</sup>). Covered entities who want their vendors to adopt and maintain what might be considered industry best practices may wish to require those vendors to commit to comply with all relevant security guidance. Business associates *may* be willing to implement existing guidance,<sup>20</sup> but many are unlikely to want to commit in advance to language that mandates adoption of unspecified standards at unknown cost.
3. Accounting for Disclosures. HITECH permits a covered entity to comply with its accounting responsibilities with respect to electronic health records by providing a complete accounting or by providing an accounting of the covered entity’s disclosures and a “list of all business associates acting on behalf of the covered entity including contact information[.]”<sup>21</sup> Parties to a BAA may or may not want to specify in advance how the covered entity will respond to future requests for accountings.
4. Responsibility for Noncompliance. Covered entities are directly accountable under HIPAA only for their own conduct and the conduct of their workforces. Yet “workforce” is defined broadly (and imprecisely) to include “employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.”<sup>22</sup> This can include temporary employees, outsourced staff, and others who may under federal and state tax and employment laws and service contracts be considered employees of a business associate but nevertheless in some respects are the responsibility of the covered entity. Moreover, many HIPAA standards that apply to a covered entity’s direct actions are implicated by a business associate’s non-compliance. For example, a covered entity that fails properly to respond to its business associate’s non-compliance with the Privacy Rule thereby may be deemed to have violated HIPAA.<sup>23</sup> For these reasons, HITECH’s enhanced enforcement provisions may cause covered entities to seek broader assurances from business associates (*e.g.*, indemnification) than previously was the case. Business associates, by contrast, are likely to seek protection for actions taken at the direction of a covered entity or its employees, and to impose other limits on potential liability to their customers (or third parties) in connection with the underlying arrangements.

---

<sup>16</sup> 42 U.S.C. §§ 17932(b) and 17934(c).

<sup>17</sup> 42 U.S.C. § 17931(c).

<sup>18</sup> 42 U.S.C. § 17932(a).

<sup>19</sup> 74 Fed. Reg. 19006 (Apr. 27, 2009). The draft guidance is available online at [http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance\\_breachnotice.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html) (accessed May 30, 2009).

<sup>20</sup> The National Institute of Standards and Technology, for example, has published *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* (Oct. 2008), available online at <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf> (accessed May 30, 2009).

<sup>21</sup> 42 U.S.C. § 17935(c)(3).

<sup>22</sup> 45 C.F.R. § 160.503.

<sup>23</sup> 45 C.F.R. § 164.504(e)(1)(ii).

Covered entities and business associates alike should work now to develop strategies for eventual compliance with HITECH. However, it remains unclear how, precisely, DHHS will implement HITECH. In addition to the security breach notification regulations required under Section 13402, HITECH instructs DHHS to amend HIPAA regulations to assure consistency with the new law.<sup>24</sup> Accordingly, regulated persons may wish to delay for some period of time actual development and implementation of new agreements or amendments, in order to avoid any duplication of effort that might be required if the eventual regulations include unanticipated provisions.

---

<sup>24</sup> 42 U.S.C. § 17951(b).