ABA Health Law Section HITECH Taskforce:

Business Associate Provisions and Templates Subcommittee

1. If Business Associate Contracts should be amended, what is the best course of action for amending: a letter amendment with new provisions? Or a new agreement?

HIPAA applies only to Covered Entities–health plans, health care clearinghouses, and almost all health care providers. However, most Covered Entities need to contract with other types of entity, which may not be Covered Entities, to perform some health care activities and functions which involve Protected Health Information. In order to extend the protections of HIPAA to Protected Health Information used by such entities, the HIPAA Privacy and Security Rules both require Covered Entities to establish Business Associate Contracts with such entities, which are called Business Associates.

A Business Associate is defined in 45 CFR§160.103 (b) as an entity that handles the protected health information of a HIPAA-covered entity and (1) provides certain functions or activities on behalf of the HIPAA-covered entity or (2) provides "legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for" the HIPAA-covered entity.

HIPAA permits a Covered Entity to disclose Protected Health Information to a Business Associate, or otherwise let the Business Associate obtain Protected Health Information to perform services for or on behalf of the Covered Entity if it obtains satisfactory written assurances that the Business Associate will use the information only for the purposes for which it is engaged, agrees to safeguard the information from misuse, and helps the Covered Entity comply with some of the Covered Entity's obligations under the Privacy Rule. This requirement is satisfied by the parties' entry into a written document that sets forth the responsibilities of the parties regarding Protected Health Information, called a "Business Associate Contract" (or sometimes Business Associate Agreement). The HIPAA regulations specify the provisions required in a Business Associate Contract, at 45 CFR§§164.314(a) and .504(e).

With the passage of HITECH the obligations of the Business Associate have changed dramatically in many respects. Section 13401(a) of HITECH -- Application of Security Provisions specifically states that most of the HIPAA Security Rule, specifically 45 CFR§§ 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards) and 164.316 (Policy and Procedures and documentation requirements) shall apply to a Business Associate of a Ccovered Entity in same manner that such sections apply to the Covered Entity. Section 13404(a) further provides that the requirements of HITECH Subtitle D, the Privacy subsection of HITECH, that "relate to privacy" which apply to Covered Entities are also applicable to Business Associates. Both HITECH sections also require that the HITECH privacy and security requirements applicable to Business Associate Contracts must be incorporated in Business Associate Contrcts. These new requirements make a Business Associate directly responsible for provisions previously applied only to the Covered Entity. At the same time, HITECH Section 13404(c) also specifies that the dramatically increased civil and criminal penalties apply to Business Associates.

The decision of how to amend current Business Associate Contracts will depend upon the complexities of the contractual arrangement between the parties and potentially the volume of

agreements at issue for a Covered Entity (or sometimes the Business Associate, as where a services vendor Business Associate has many Covered Entity clients) . Many of the Business Associate Contracts currently used provide that the parties will agree to abide by all future amendments of the HIPAA Privacy and Security Rules, or have language to such effect, which may be sufficient for compliance until a more formal document can be negotiated and prepared. Even where such language exists, however, both parties might often benefit from a well thought out exchange that could memorialize their understanding of the responsibilities and duties mandated by HITECH.

Some commenters have suggested that a letter amendment sent by one party to the other will suffice to memorialize the new obligations. While this may be true, most contracts provide that any amendment to the agreement must be signed by both parties to be enforceable. If so, the parties will still need to prepare an amendment, at a minimum, which must be signed by both parties.

Other commenters have suggested that a new Business Associate Agreement must be drafted and signed by all parties. Certainly, this is the approach recommended for all new Business Associate arrangements. However, additional regulatory guidance is expected some time during the next several months and could impact the strategy or legal obligation of the parties. Any new agreement or amendment to an existing agreement must take that reality into consideration when deciding how to move forward with the new regulatory compliance mandated by HITECH.

2. What is the deadline for amending Business Associate Agreements? Will the Office for Civil Rights issue model Business Associate Contracts?

There are many rumors regarding when and if the OCR will issue any guidance on whether Business Associate Agreements are required to be amended and, if so, how to amend them to comply with HITECH. However, no official announcements have been made. An OCR official reportedly stated publicly that there would be guidance and an updated model Business Associate Agreement, but not until February 2010, and that there would be an enforcement "grace period." However, the lack of an official pronouncement makes it prudent to proceed with compliance efforts based on the deadlines provided in the law itself.

The general effective date for HITECH is February 17, 2010. This is also the specific deadline applicable to sections 13401(a) and 13404(a) of HITECH, the sections requiring the "incorporation" of certain provisions into Business Associate Agreements. Therefore, those interpreting the law to require amendment of Business Associate Agreements argue that they need to be amended by this date.

Note, however, that different HITECH provisions have differing compliance deadlines, many of which are dependent on the promulgation of regulations. For example, the security breach notification requirements are technically already effective, but HHS stated that it will use its "enforcement discretion to not impose sanctions for failure to provide the required notifications for breaches that are discovered before . . . February 22, 2010." 74 Fed. Reg. 42757 (Aug. 24, 2009).

3. Should Business Associate Agreements reflect HITECH's new security breach notification and reporting requirements? What factors should Covered Entities and Business Associates consider when drafting these provisions?

Section 13402 of HITECH applies to both Covered Entities and Business Associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured Protected Health Information and requires them to make certain notifications following a discovery of a breach of unsecured Protected Health Information. There is no specific statutory or regulatory mandate to incorporate these notification requirements into Business Associate Agreements, though the requirements of HITECH Sections 13401(a) and 13404(a), requiring the "incorporation" of HITECH requirements into Business Associate Contracts suggests it would be prudent to reference them at least.

There are also several other reasons why many Covered Entities and Business Associates will feel compelled to include provisions regarding these notification requirements into their Business Associate Agreements.

- The breach notification requirements can involve significant monetary costs. Not only does HITECH provide significant monetary penalties for noncompliance with the notification requirements, but compliance with the requirements can be very costly as well, particularly in regard to the Covered Entity's obligation to notify individuals. Even where a Business Associate is responsible for the breach, the law requires the covered entity to make these potentially expensive notifications.

  In order to protect themselves from the high penalties for noncompliance, many Covered Entities and Business Associates will want to include provisions in their Business Associate Agreements requiring the party responsible for the breach to indemnify the other party or otherwise allocating such liability. In addition, many Covered Entities will likely want their Business Associate Agreements to obligate the Business Associate to shoulder at least part, if not all, of the costs and/or responsibility for the notifications where the breach was caused by the Business Associate.

  - The required notifications can have a significant impact on an organization's public image. Covered Entities are legally required to notify individuals, HHS, and in some cases, the media, about the breach. Even in cases where a Business Associate is solely responsible for the security breach, the Covered Entity is still the party legally obligated to make these notifications. Since the Covered Entity's notification can include an unflattering portrayal of the Business Associate, particularly in cases where the Business Associate is responsible for the breach, many Business Associates will want to retain control over the content of these notifications to the greatest extent possible. Business Associates will justifiably be concerned about how they are portrayed not only in the Covered Entity's notifications to individuals and to the media and the concomitant potential affect on its public image, but also in the Covered Entity's notification to HHS since HHS may impose monetary penalties on the Business Associate for failure to have adequate security measures in place to prevent such breaches. In fact, the security breach notification form that Covered Entities are required to use to report breaches to HHS requires Covered Entities to provide information about any Business Associates that were involved in the breach. Business Associates are likely to want their Business Associate

Agreements to give them some measure of control over the content of the notifications made by Covered Entities.

- Covered Entities may not want to rely on their Business Associates' judgment as to whether the breach notification provisions apply. Even though the breach notification requirements are separately and directly applicable to Covered Entities and Business Associates, Covered entities rely on their Business Associates to the extent that Covered Entities are required to make certain notifications when their Business Associates experience security breaches. HITECH requires a Business Associate to notify the Covered Entity when the breach involves the Covered Entity's Protected Health Information and the Covered Entity, in turn, must then make additional notifications to individuals, HHS, and/or the media, depending on the circumstances. In fact, where the Business Associate is the Covered Entity's agent, as opposed to independent contractor, the Covered Entity's notification obligations are triggered based on the time that the Business Associate discovers the breach, not the time that the Business Associate notifies the Covered Entity. 74 Federal Register 42754 (Aug. 24, 2009). If the Business Associate does not inform the Covered Entity of the breach, the Covered Entity will be unable to comply with its notification requirements and can potentially be subjected to investigation and the imposition of penalties.

  Yet, HITECH does not require Business Associates to report all security breaches to Covered Entities. In order to determine if notifications are required, HITECH sets forth a detailed analysis, which includes a risk assessment and the application of subjective judgment. In many cases, a Business Associate may conclude that HITECH does not require it to notify the Covered Entity about the breach. However, the Covered Entity may not agree with the Business Associate's analysis and, therefore, many Covered Entities are likely to want their Business Associates to inform them of any security breaches involving their Protected Health Information so that they can undertake their own analysis of whether any notification requirements apply. HIPAA already requires that Business Associate Contracts obligate the Business Associate to report security incidents to the Covered Entity. 45 CFR 164.504(e)(2)(ii)(C) and 164.314(a)(2)(i)(C). It is in the Covered Entity's interest to ensure that its Business Associate Agreements very clearly and broadly set forth when the Business Associate must notify the Covered Entity about a breach or potential breach.

As mentioned above, Business Associate Agreements may not be specifically required to be amended to reflect HITECH's new notification requirements. Nevertheless, Covered Entities and Business Associates would be prudent to include such provisions in their agreements to protect their rights and interests. Depending on the size, complexity, and other particular circumstances of the Covered Entity or Business Associate, the parties to the agreement may have the concerns outlined above or others as well. In its interim final rule on breach notification, HHS stated:

> [W]e emphasize that we do not intend for this section to interfere with the current relationship between covered entities and their business associates. Business associates and covered entities will continue to have the flexibility to set forth specific obligations for each party, such as who will provide notice to individuals and when the notification from the business associate to the covered entity will be required, following a breach of unsecured protected health information, so long as all required notifications are provided and the other requirements of the interim

> final rule are met. We encourage the parties to consider which entity is in the best position to provide notice to the individual, which may depend on circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual. We also encourage the parties to ensure the individual does not receive notifications from both the covered entity and the business associate about the same breach, which may be confusing to the individual. 74 Federal Register 42755 (Aug. 24, 2009).

Covered Entities and Business Associates, therefore, should consider these factors and determine what rights they might want and what obligations they might want imposed on the other party and negotiate their Business Associate Agreements accordingly.