

## **Business Associate Agreements: Key HITECH Changes to Consider June, 2010**

*Leslie Ann Fox, MA, RHIA, Patty Thierry Sheridan, MBA, RHIA*

*Thank you to Advance Magazine for permission to use this article*

LESLIE: When the HITECH act was signed into law on Feb. 17, 2009, as part of the American Recovery and Reinvestment Act of 2009 (ARRA) it reshaped the regulations around privacy and security. In particular, business associates (BAs) are now regulated directly rather than indirectly through a covered entity to comply with privacy and security requirements.

PATTY: I think this change requires new ways of thinking about the BA Agreement (BAA).

LESLIE: How so?

PATTY: Because BAs are regulated in the exact same way as covered entities (CEs), managing breach notification, risk mitigation and accounting of disclosures become shared responsibilities in a way that didn't exist before HITECH. Let's include Gwen Hughes, Care Communications' privacy officer and e-HIM practice line director, in our conversation today to expand on this idea more fully. Gwen, what is the current state with regard to BA changes and by extension BAAs?

GWEN: At this point we have interim final rules related to breach notification and enforcement to which CEs and BAs are both subject. Draft guidance on risk analysis has also been published.

There are more rules coming, however. The Office for Civil Rights will implement important privacy and security provisions of the HITECH Act through the Notice of Proposed Rulemaking (NPRM) process. Subjects that CEs and BAs expect to hear more include: BAAs; BA liability; limitations on the sale of protected health information (PHI), marketing, fundraising and communication; the accounting of disclosure; minimum necessary; and stronger individual rights to access electronic health information and to restrict disclosure of information. Although these provisions of the HITECH Act are already in effect, future NPRM(s) should provide guidance on implementation and enforcement.

LESLIE: Do CEs and BAs need to update their BAAs?

GWEN: That is a good question and is causing a bit of confusion. The HITECH Act says that the HIPAA privacy and security requirements shall be incorporated into the BAA between the BA and the CE. There is disagreement among attorneys about what this means exactly. Some attorneys interpret the requirement to mean that the BAA must list the HIPAA privacy and security requirements to which the BA is subject. For example the BAA might require the BA to use appropriate safeguards, maintain a record of disclosures, report unauthorized uses or disclosures, etc. Others think the requirement means the BAA must include specifics, such as requiring an encryption protocol when transmitting PHI across the Internet during the coding process.

LESLIE: This seems resource intensive for both CEs and BAs. It's not inconceivable for a CE to have several hundred BAs in place and vice versa.

GWEN: That is true. We could be talking about making changes to hundreds of BAA agreements for one CE or one BA initially and perhaps the same number of changes or amendments annually thereafter. Given there are still rules pending, I am not so sure this is the best way to go.

PATTY: What are other options?

GWEN: Some health care attorneys argue that because HITECH directly imposes on BAs the privacy and security requirements under HIPAA and as amended under HITECH, it is unnecessary to update existing BAAs.

I think it may depend on the wording of the existing BAA. If the existing BAA says that the BAA will have to be amended periodically to reflect changes to HIPAA, the BAA will probably need to be amended. On the other hand, if the BAA requires the BA to comply with HIPAA and to incorporate amendments or revisions to HIPAA necessary to assure ongoing compliance, there may not be a need to update the BAA.

It will be interesting to see what guidance the federal government provides. I do think it makes sense for CEs to require BAs to adhere to the CE's most recent policies on privacy and security. It will then be the responsibility of the CE to share their privacy and security policies with the BA and to talk through any problems the BA will encounter. Such a conversation may need to occur around the time of contract signing or when there is a substantial change in policy. The BA would train their staff on the CE's privacy and security practices. This would ensure that the BAA between the CE and BA reflects the evolution in practice without having to constantly issue another BAA addendum.

LESLIE: So what you are suggesting is that all BAAs be updated as needed to include language where the BA must comply with current HIPAA privacy and security rules, regulations and guidance, and the CE's most recent privacy and security policies. Is there anything else?

GWEN: Yes, I think that BAAs should include the position and contact information for the individuals to be contacted for the CE and BA in the event a breach should occur. The timeframe for contacting that individual should also be included. The Breach Notification rule currently says the BA must provide notice to the CE without unreasonable delay and no later than 60 days from the discovery of the breach. The longer the BA takes to communicate, the more stressful the situation could become for that CE, which also has certain mitigation and reporting responsibilities. CEs may want to request the BA report a potential breach to the CE within 48 hours, for example. I think the CE should know as soon as possible about a breach, as well as the status of the investigation.

I also think that it would be helpful to include a breach mitigation strategy in an updated BAA as well.

PATTY: What does a breach mitigation strategy mean exactly?

GWEN: In the past if there was a breach, the BA reported the breach to the CE and the CE would take it from there. Under the HITECH revisions to the privacy and security rule, this should be a collaborative effort. A breach is a naturally anxious experience for both parties and there could be a tendency to be reactive and blaming while trying to protect the reputation of one's own organization. I think it is wise to outline the sequence of steps that will take place in the event of a breach and who will be at the table from the CE and BA. Both parties have a lot at stake, and risk mitigation efforts must be in concert.

Another possibility is to have a neutral third party to help both organizations. Given how really anxious and often emotional this kind of situation can become for all parties involved, a neutral third party that is not involved, can ensure actions are taken in the best interest of the patients and the CE and BA.

PATTY: There needs to be some level of trust in the other that each organization will manage their anxiety and move swiftly and responsibly. And ideally, emerging stronger in their partnership rather than dissolving the partnership.

LESLIE: What else should be included in the BAA update?

GWEN: I think CEs and BAs should consider including an escalation policy so that if the CE thinks the BA is not adhering to the HITECH act or vice versa, they know how to address that concern.

LESLIE: That implies that the CE or the BA can report the other?

GWEN: Yes, under the privacy regulations, guidance and the HITECH Act, the CE and BA are obligated to report one another when one knows the other has committed a material breach of HIPAA and reasonable steps to cure the breach, end the violation and/or terminate the BAA are not possible. In such cases, the CE or BA must inform the Secretary of Health and Human Services (HHS). Failure to report is a violation of HIPAA. Preferably it never comes to this and both parties learn from the other and are open to discussion, but I believe there should be an understanding about how differences of opinion will be addressed.

PATTY: I understand that the HITECH Act requires HHS to conduct compliance audits. Are these announced visits?

GWEN: The HITECH Act authorizes the Secretary to conduct periodic compliance audits of CEs to ensure they are in compliance with HIPAA, as amended by the HITECH Act. Details about the number of audits, frequency of audits on a single CE, and whether there will be advance notice are unknown as of now, but may be detailed in future regulations.

LESLIE: To recap then, the most important revisions to the BAA are:

- Reference in the BAA that the BA will comply with the most current HITECH privacy and security rulings and the CE's privacy and security policies
- Inclusion of key contacts in the event of a potential breach and the time frame in which to contact those individuals
- Inclusion of a mitigation strategy which outlines the steps the CE and BA will take in the event of a potential breach
- Inclusion of an escalation process in the event noncompliance becomes an issue

GWEN: Yes, these are the most striking changes to consider when updating a BAA from my perspective.

PATTY: What about accounting of disclosures? I understand this will expand to include uses and disclosures for treatment, payment and health care operations (TPO). Is there anything that needs to be included in the BAA in this regard?

GWEN: Not at this time. There is an expectation that CE EHR software will automatically track all uses and disclosures including those for TPO. BA uses and disclosures including those for TPO will need to be tracked on the accounting of disclosures as well.

LESLIE: How is that going to be tracked? Through EHR audit trails?

GWEN: EHR audit trails are not currently designed to support accounting of disclosures. For example, an audit trail does not include the purpose of disclosure, which is an important data element in the accounting of disclosures. A CE and their BAs will need to dialogue on how to best meet this requirement. The HITECH Act provides that a CE that has acquired an EHR after Jan. 1, 2009 must comply with the new accounting requirement beginning Jan. 1, 2011 (or anytime after that date when it acquires an EHR), unless the government extends the date until 2013. The government just closed a public comment period on this subject May 18.

I think most CEs will find they need their EHR software to track uses and disclosures by their Bas, but that they need to develop codes to enter on behalf of certain users that will automatically populate accounting of disclosure fields, such as “coding” or “transcription”: as the purpose of the use or disclosure whenever that individual accesses a record as part of their contract.

PATTY: How does one stay current on all of these changes?

GWEN: There are a number of resources but the one’s I tend to keep abreast of are as follows:

- HHS Website with up to date information on NPRM and interpretation of the regulations;
- AHIMA’s one stop resource for all things ARRA and HITECH;
- ONC’s update on HITECH, which includes timelines for privacy and security regulations;
- HHS’s updates on HIT initiatives; and
- National Institute of Standards and Technology -- Advancements in technology state of art.

LESLIE: Is there anything else we should have on radar for now?

GWEN: BAs should be considering three additional items:

1. BAs need to perform a privacy and security gap analysis and risk assessment if they didn’t already when HIPAA first went into affect. This means going through each standard and determining if it applies to the BA and if so confirming compliance.
2. BAs need to become conversant on state laws. There are 42 state laws with breach notification requirements. That suggests for example if a BA has a breach that includes individuals from various states, they will need a state-by-state breach strategy.
3. BAs should review their errors and omission insurance to understand what is covered and what is not should a breach occur.

PATTY: Thank you Gwen for all this helpful information. You have given us a lot to consider and an understanding of how important it is for CEs and BAs to work collaboratively in the best interest of patients and each organization.

---

*Leslie Ann Fox is chief executive officer and Patty Thierry Sheridan is president of Care Communications Inc., a national HIM consulting and staffing company headquartered in Chicago. They invite readers to send their thoughts and opinions on this column to [lfox@care-communications.com](mailto:lfox@care-communications.com) or [ptsheridan@care-communications.com](mailto:ptsheridan@care-communications.com).*