BY CHRISTINE P. ROBERTS

HITECH's impact on brokers and advisers

Any health benefit broker or adviser can attest to how significantly the compliance landscape changed when HIPAA was enacted back in 1996. Unfortunately, recent amendments to HIPAA represent almost as significant a change to the status quo as HIPAA did back then.

These amendments were contained in the Health Information Technology for Economic and Clinical Health Act of 2009, which was part of the economic "bailout bill" enacted in February 2009.

IMAGE BY DAVID LEONARD

The "HITECH" law changes benefit brokers' and advisers' worlds in two ways:

- It requires business associates to notify covered entities of a breach of "unsecured" protected health information that occurs on their watch.
- It upgrades all business associate duties under HIPAA to those of a covered entity.

With regard to breach notification duties, a business associate must notify a covered entity of any breach of unsecured PHI pertaining to one or more of the covered entity's participants or insureds. Notice must be provided "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach." To the extent it is available, and in the same time period, the business associate must also provide the covered entity with information that will permit the covered entity to notify the individuals affected by the breach and take other corrective steps.

The regulations define the terms "breach" and "unsecured" to include certain carve-outs. For instance, "unsecured" PHI is unencrypted PHI, and encrypted PHI cannot be breached. Similarly, the term "breach" does not include certain unintentional, good-faith disclosures.

These new HITECH responsibilities present several issues regarding business associate agreements. The first is how much time the business associate will have to notify the covered entity after discovery of a breach (or the point at which a breach would have been discovered through the exercise of due diligence). Insurers are being very aggressive in this regard, allowing only three business days for notice. I recommend that business associates agree to notify the covered entity of the fact of the breach within that time period — or a similarly brief one — but bargain for additional time to provide specific information on the breach, such as a description of how it happened, who was affected, etc. Depending on the circumstances, of course, this may or may not be possible.

A second drafting point is that a BAA which characterizes the business associate as an "agent" of the covered entity will share a single 60-day notice period with the covered entity, while using "independent contractor" terminology provides the business associate with its own 60-day period to notify the covered entity. Of course, the agent/independent contractor designation should be driven by the facts of the relationship and not by the desire to have additional notice time; business associates with questions in this regard should consult their compliance counsel.

Brokers and advisers that use their own BAAs with clients should update those BAAs to incorporate their HITECH responsibilities in a way that is is most protective of their interests and limits their duties as much as possible.

Finally, with regard to the upgrade of business associate HIPAA duties to those of a covered entity, taking a proactive stance may give you a marketing edge over competitors who are taking a "wait and see" approach. However, beware of blindly imposing a full HIPAA compliance regime before doing a self-audit that identifies how your organization obtains, creates, uses and discloses PHI. There is no point in committing to safeguards or procedures that are not relevant to the services or functions you fulfill. **EBA**

Roberts is a partner in the law firm of Mullen & Henzell LLP in Santa Barbara, Calif. She can be reached at croberts@mullenlaw.com.