HIPAA Regulations & Business Associates

By John Landreth, CPA

Welcome to this issue's *Letters to the Auditor*. In this issue, we hear from a reader who has questions about the HIPAA regulations concerning Business Associates (BA).

Dear Letters to the Auditor,

Thanks for the excellent HIPAA diagnostic tool in the last issue. We have finally seen the light. We are moving ahead. There's only one stumper....

What's all this business about associates in these HIPAA regulations or that is Business Associates in HIPAA? My hospital has thousands of vendors of some sort of another - how do you sort them all out? They are all alike - they all want our money.

Then there's "Chain of Trust" (COT) agreements I am also hearing about. Sounds like a country western song of some kind. Will auditors in the future see their CEO on the 10 o'clock news wearing handcuffs because they did not have a COT agreement?

How do you tell the difference between a Business Associate and a COT partner? Will we have tearful announcements with our vendors in the future where we say "Oh, I am sorry, Mr. Vendor, but you are not going to be a Chair of Trust Partner I can only work with you as a friend... eh, a Business Associate, that is."

Lastly, if my trusted COT partner or BA decides to go "postal" with my patient health information, who's the one at risk? Is my organization insulated from the liability of their actions? Are we obligated to conduct further due diligence with this vendor to make sure they share the same concern for privacy and are living up to their agreements?

HIPAA Harried

Dear HIPAA Harried,

As you may or may not know, the final modifications to the HIPAA Privacy Regulation were published in the *Federal Register* on August 14, 2002. According to the federal government, it will not make any further regulatory changes (though they do hope to release additional guidance) prior to the April, 14, 2003, compliance date. Covered entities now know what they have to do to become compliant with the HIPAA privacy regulation.

The privacy regulation states that a BA is a "person or entity" who performs a function or activity on behalf of a healthcare organization "involving the use or disclosure of protected health information" (PHI). Therefore, the covered entity, beyond making sure its "shop" is in order, is also required to impose, through contracts, the privacy standards of the Privacy Rule on parties who access and use PHI to perform certain services on its behalf.

According to the regulation, examples of BA activities that involve PHI include claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Other BA activities may include the disclosure of PHI include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

However, it is important to remember that the rule includes exceptions. The BA requirements do not apply to covered entities who disclose PHI to providers for treatment purposes - for example, information exchanges between a hospital and physicians with admitting privileges at the hospital. And, for those companies that provide certain services (i.e., construction, courier, janitorial, delivery, and maintenance) that don't involve the use or disclosure of PHI, are not considered a BA. The covered entity is responsible to ensure that incidental exposure of PHI to these companies or people is limited through reasonable safeguards.

The bottom line is that you have to begin (if not already) to identify all your BAs and develop a strategy to incorporate the necessary BAs provisions in your contracts. Bob Gross, HIPAA Project Manager, at Northwestern Memorial Hospital (NMH) says, "This is an extremely laborious process that involves participation from and coordination with the hospital's legal department, materials/ contracts management, account payable, and departmental managers."

Gross adds, "It is no surprise that information privacy and security touches every aspect of the hospital, but dealing with BAs is a little different. We recognized that we must start the BA project early because we are dealing with entities that

are not directly under our control (i.e., employees). It requires a well-thought out approach that builds in a lot of time for the negotiation process. The unknown factor that concerns me is how long will the contract negotiation process last. Apparently, the government echoes that sentiment and has given us a reprieve."

Well, NMH did start relatively early and, in February 2002, its accounts payable department produced a report reflecting vendors that received checks during fiscal year 2001 (September 2000 – September 2001). The report was sorted by the manager of each cost center and a "vendor survey" was then distributed to them to complete. The survey questions were:

1. Does the current written contract with NMH expire before April 13, 2003?
2. Does the vendor perform a function, service, or activity that uses PHI?
3. Does the vendor perform as an NMH employee, volunteer, trainee, or someone under the direct control of NMH?
4. Does the vendor perform as a **physician** or person with staff privileges who provides services to or for patients of NMH?
5. Does the vendor perform as a **health plan** where PHI is disclosed to or for enrollees or on their behalf?
6. Does the vendor perform as a **governmental agency**?

An analysis of the survey responses was performed (some follow up was necessary) to determine which vendors were indeed BAs. The magic combination of *No, Yes, No, No, No, No* indicated that the vendor is a NMH BA under the privacy regulation. NMH estimates that it has roughly 300 business associates for which BAs addendum language must be included in the existing contracts and negotiated with vendors by the April 14, 2004, deadline.

However, this estimate does not include new vendors that came on board after September 2001. At the time this article was written, NMH is analyzing data from September 2002 to the present to identify additional vendors that would also be considered BAs.

NMH's legal department drafted a BA addendum which is to be included with both old and new contracts, to reflect the BAs obligations and expectations. A tracking mechanism will soon be developed to track the contract negotiation progress. The process will be managed by NMH's Materials Management Department and will be audited by NMH's Internal Audit Department.

I should point out, that the covered entity is not totally off the hook once a BA agreement is in place. Under the final regulation, the covered entity needs to obtain assurances that the BA will safeguard PHI it receives. I am not saying you have to knock on their door and actively monitor their performance. However, if you learn of their breach, you must require the BA to cure the breach.

It is really important to exercise reasonable due diligence in selecting any vendor, regardless if they use and disclose PHI. Failure to do so may expose the covered entity to become the victim of criminal behavior - such as fraud, double billing, and substandard service. You should get to know your BAs and feel comfortable with their commitment to protecting your PHI.

As far as seeing CEOs on the news in handcuffs, I don't think that is going to happen. The federal government recently announced that the Department of Health and Human Services' Office of Civil Rights will be enforcing the privacy regulation. Enforcement activities will focus on obtaining voluntary compliance through technical assistance. The process will be primarily complaint driven and will consist of progressive steps that will provide opportunities to demonstrate compliance or submit a corrective action plan. So, the good news is that the HIPAA "police" won't come banging on your door unannounced, but may get involved if a complaint is filed.

If you are worried about how you look in pinstripes (and I mean not the ones you find at Brooks Brothers), I guess those pinstripes would be made for folks who commit wrongful disclosures of PHI with the intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm. If you are up to no good then you deserve what you get.

Now, on to the COT agreements. Hopefully, this response will relieve your anxiety. COT agreements are the security equivalent of BAs. They can be fairly technical because they outline the specific security measures that entities sharing and exchanging PHI will use to protect the integrity of information. A lot of people are using the words "chain of trust" when they really mean BA agreement. You won't find the words chain of trust in the privacy regulation, and the security regulation isn't finalized. However, the rumor is that it will be published in late December 2002.

Because the security regulation is not final, it really is not necessary to ask BAs to sign COT agreements. We don't know yet what to include in the document. You never know, the federal government may provide guidance on how to handle this dilemma. However, if you feel that you must do something, one suggestion is to incorporate language in your BA contracts that allow you to add chain of trust agreements once the security rule is finalized. Hey, if this means you will sleep better at night then do it. ■

Well that's all for this issue of *Letters to the Auditor*. Please keep your letters, faxes, e-mails coming in. We'll see you next time.

A very special "thank you" to Bob Gross for his very informative, thorough and expert advice and help with this issues column. If you have questions regarding the HIPAA regulations, contact Bob at (312) 926-5341.

Remember:

Mark your calendar for the 2003 Annual Conference .. September 14-17, 2003, Disney Coronado Resort, Florida