Billing
Healthcare Billing & Management Association

HBMA

March/April 2003

HIPAA for Billing Companies Business Associate Agreements

With the April 14, 2003 HIPAA Privacy Rule deadline, providers and other Covered Entities should have the applicable HIPAA requirements developed and in place. One such requirement under the HIPAA Privacy Rule is for Covered Entities (CEs) to obtain a written agreement that contains privacy and security assurances from its Business Associates (BAs). Although the previous sentence seems straightforward enough, it begs (at least) two questions:

1. What or who is a Business Associate?
2. What kinds of assurances need to be included in the written agreement?

While April 14, 2003 is the deadline for Privacy Rule compliance, there is a two-part deadline for BA agreements.

This article will help you in finding answers to those questions and should give you a basic outline for compliance with this HIPAA requirement. *(A note: while this is written as an aid to understanding the HIPAA requirements for Business Associate agreements, it is not intended as, nor should it substitute for, legal advice. Always seek the counsel of a qualified attorney when drafting or reviewing contracts and other legal documents.)*

TIMING/DEADLINES

Before discussing the answers to the two questions above, timelines for this requirement should be explained. While April 14, 2003 is the deadline for Privacy Rule compliance, there is a two-part deadline for BA agreements. After April 14, 2003, all **new** relationships between CEs and their BAs will need to be in writing, and include all the requisite assurances for privacy and security. This applies to **new** relationships or new contracts only. For **existing** relationships on or before April 14, 2003 the deadline may be different. If there is an existing written contract between the CE and the BA that does not come up for renewal until after April 14, 2003, then the HIPAA assurances may be added to the contract at its annual renewal time. If the contract is "evergreen" or for multiple years, then the HIPAA provisions must be included no later than **April 14, 2004**. In short, the deadline for having the required HIPAA privacy agreements in place may be as late as *April 14, 2004,* if the relationship is already covered by an existing contract between the Covered Entity and the Business Associate.

WHAT OR WHO IS A BUSINESS ASSOCIATE?

Let's go back to the first of the two questions above. A Business Associate relationship exists when an individual or entity (other than an employee), acting on behalf of the Covered Entity, assists in the performance of a function or activity involving the use or disclosure of Protected Health Information (PHI). This may include services such as legal, accounting, administrative, actuarial, consulting, management, financial or others. For example, a billing service or practice management company is going to be a BA for its provider/clients. That one's easy, and for some HBMA members, may be the only type of BA agreement that concerns them. We will *(continued on page 4)*

INSIDE...

(HIPAA continued from page 1)

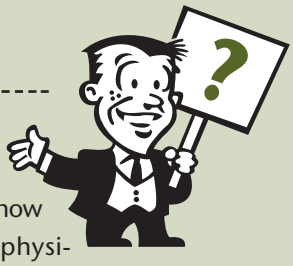
focus here on those types of agreements, but there are other situations that should also be mentioned briefly.

For those billing companies and practice management organizations which are Covered Entities in their own right, by virtue of being a healthcare clearinghouse or otherwise, there may be a wide range of relationships that will necessitate a Business Associate agreement. In addition to the services listed in the previous paragraph, the following are examples of functions and services that should be considered as well:

- document imaging/scanning
- document storage and retrieval
- software vendors/programmers
- auditors
- mailing services
- collection agencies (may be BAs of the client and/or the billing company)
- document destruction
- coding contractors
- independent or sub-contractors for a variety of internal functions
- call centers
- certain insurance carriers

(continued on page 10)

Question of the Month



Q. With the recent Medicare cuts, some physicians are interested in eliminating new Medicare patients and only taking care of existing patients or they want to schedule fewer new Medicare patients. All of my physicians consider compliance issues as a top priority. What advice should I give them?

A. There have been an increasing number of stories published lately about providers closing out their Medicare practice, reducing the number of Medicare patients, etc. Most of the coverage has cited the recent payment cuts and the prospect of additional cuts in the next few years that add to the mounting 'hassle factor' of dealing with the Medicare program.

Simply put, in a free society, providers are in complete control of whether they accept any new patient(s), how many (or none) from any category, and whether they keep any, some, or selected existing patients. For example, for decades some practices have elected not to serve Medicaid patients, or to 'budget' a volume of Medicaid patients because of the pittance paid by those programs. Some specialists are even refusing to perform certain services (CPT-4 level) because of under-compensation.

TWO ITEMS OF CAUTION:

1. Every state has laws governing 'abandonment.' That means that a patient has the right to expect ongoing care, particularly if he or she is under 'active treatment' UNLESS the provider gives them advance notice of the provider's termination of the relationship. This is particularly important for specialists.

The amount of notice required varies by state. Most states also require that the current provider make 'reasonable' efforts (not extraordinary efforts) to assist the patient in locating an alternate provider. Although many practices elect to accomplish this through attrition, it is legal to 'prune' the practice if it is done according to state law and as long as no patient's life is jeopardized.

2. Be mindful of EEOC laws. If a practice must make difficult financial decisions, it should be thoughtful about whether these decisions produce something that looks like (or is) 'red-lining' or 'profiling' of the ugly type. Certainly, if the practice (or you, on their behalf) has developed any financial analysis (it's not required) that supported the decision, that would be helpful.

Thought must also be given to how to handle physicians who take their turn "on call" for their hospital's Emergency Department and/or Trauma Center. They would have to take ANY new patient, but could inform the patient that the practice is limited and they will have to refer the patient after discharge.

FINAL THOUGHTS: Last year, the OIG made a big deal about a conference speaker (alleged to be a consultant) who told doctors to drop Medicaid and/or Medicare patient volumes to make their practices more profitable. The OIG inferred (but never said, because it would be untrue) that this was somehow improper. It isn't, never has been, and never will be.

Get a qualified healthcare lawyer to review any letters to be used to notify patients and don't be bashful about saying why this is happening.

Training your staff and the practices' staff will be important, since proper patient handling will matter.

Bob Burleigh CHBME, is President of Brandywine Healthcare Services. He can be reached at brandywinebob@aol.com

(HIPAA continued from page 4)

Not all of the providers of these services will necessarily be Business Associates of a billing or practice management company that is a Covered Entity, but they represent the types of contractors and agents that may be.

WHAT SHOULD A BUSINESS ASSOCIATE AGREEMENT INCLUDE?

Once you have determined who or what is a Business Associate as far as your organization is concerned, and as you draft an agreement between you and your clients, or review an agreement that has been submitted for your signature, you can use the following checklist to see if all the required and/or recommended provisions are included.

Identification and Definition. As with any well-written contract, the parties should be clearly identified, and all specific terms should be defined or have their definition referenced. For a HIPAA BA agreement, this could mean that when terms such as *PHI, information, data* or similar words are used they should be specifically defined or have the same meaning as set out in the HIPAA Privacy Rule itself. There will also be boilerplate language about choice of law (in what State will any disputes be heard?), indemnity clauses, survival of confidentiality terms, termination, and others. Remember: it is very important that you seek out appropriate legal advice from a qualified attorney to make sure that all the clauses relevant to your situation are included and properly drafted.

Responsibilities. If the BA agreement is a stand-alone contract, it must include the responsibilities of both the Covered Entity and the Business Associate, and clearly state what the functions to be performed by the BA will be, as well as the required assurances. If the BA agreement is an addendum to or part of an existing contract, then the underlying agreement should be referenced as to the duties and responsibilities of each party. Either way, the following items should be included in any agreement drafted for compliance with the HIPAA Privacy Rule. The Business Associate should agree to:

- Not use or disclose the information (PHI or other defined term), other than as permitted or required by the agreement or required by law.
- Use appropriate safeguards to prevent use or disclosure other than as permitted by the agreement (security).*

Read any agreement you are asked to sign very carefully, with an eye to how it would operate in the "real world."

- Ensure that agents and subcontractors to whom it provides access to the information agree to the same privacy (and security) restrictions applicable to BA.*
- Report to the CE any use or disclosure of PHI which the BA learns that is not permitted by the agreement (or any security incident).*
- Mitigate, to the extent practicable, any harm from a use or disclosure of PHI in violation of the agreement.
- Make the information available for individuals' access, disclosure accounting, and amendment as directed by the CE and incorporate any appropriate amendments received from the CE (it is important for the two parties to work out very carefully as to how the patients' rights will be addressed).
- Upon advance written notice and during normal business hours, make internal practices, books, and records relating to the use and disclosure of the information received by the CE, or created or received on behalf of CE, available to the CE and/or the U.S. Department of Health and Human Services for purposes of determining the CE's compliance with the Privacy Rules.
- At contract termination, return or destroy, if feasible, all protected health information received from or created or received for CE. For protected health information not feasible to return or destroy, limit its further use and disclosure to those purposes that make return or destruction infeasible.
- Authorize contract termination if the CE determines that the BA has violated a material term of the contract.

(See paragraph below)*

The newly-finalized **HIPAA Security Rules** also have requirements for contract assurances relating to the safeguarding of electronic health information. In contrast to the proposed Security Rule, the final rule says that these requirements can be included in the BA agreement rather than in a separate "chain of trust" agreement. The three required areas overlap with certain of the BA requirements (marked with an *, above), and must say that a Business Associate will:

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the CE's electronic protected health information.
- Ensure that its agents and subcontractors to whom it provides the in-

formation do the same.
- Report to the CE any security incident (security breach or unauthorized disclosure) of which it becomes aware.

When drafting or reviewing a Business Associate agreement that your billing or practice management company is to sign, there are a couple of other things that you should ensure are included and that you are comfortable with. First make very sure that the agreement explicitly states that you as the Business Associate may use or disclose PHI to perform functions, activities, and services for, or on behalf of, the Covered Entity as specified in any applicable contracts between the CE and BA. The agreement should also include language enabling the Business Associate to use and disclose the information for the proper management and administration of the BA's business, or to carry out its legal responsibilities. These types of clauses were glaringly absent from some early versions of BA agreements sent out *en masse* by a certain large hospital chain and may have rendered them inoperable and most likely unenforceable. Read any agreement you are asked to sign very carefully, with an eye to how it would operate in the "real world."

WHAT ABOUT RECIPROCAL AGREEMENTS?

There may be some situations where the parties to a contractual relationship are both Covered Entities and Business Associates to each other (e.g., a billing company and true clearinghouse, in certain instances). When this is the case, there does not need to be two separate agreements. One agreement, carefully drafted and acceptable to both sides, is often preferable for reasons of efficiency and ease of enforcement. The provisions discussed above should be included, as well as any others that your legal counsel recommends, but the parties may be referred to by such titles as Receiving Party and Disclosing Party (rather than CE and BA), so that each clause could apply to either party to the agreement.

ARE THERE EXCEPTIONS TO THE BUSINESS ASSOCIATE REQUIREMENT?

As mentioned above, **employees** of Covered Entities do not have to enter into Business Associate agreements with the CEs under the HIPAA Privacy Rule standards. There are other notable exceptions to this requirement as well. No agreement is necessary between two CEs/providers to enable them to share PHI for **purposes of treatment** of a mutual patient. Other arrangements between two CEs/providers may require a BA agreement: for example, a medical group and a hospital who enter into a shared risk pool arrangement would both be BAs to each other for that purpose. CEs/providers can also enter into **organized health care arrangements** that do not require Business Associate agreements between them.

On April 14, 2003, the requirements for these agreements begin to kick in, and by April 14, 2004, every relevant relationship should be compliant with these requirements.

No Business Associate agreement is necessary between a CE and a **financial institution** if the institution processes only consumer-conducted transactions for purposes of payment for health care services. A bank that clears checks for a CE would not be considered a BA. However, a bank that operates a lock-box arrangement or receives electronic EOBs as well as payments on behalf of a Covered Entity would most likely require a BA agreement.

Disclosures between a **group health plan and the plan sponsor** (usually an employer with a self-funded insurance plan for employees) do not require a Business Associate agreement according to HIPAA. However, there are specific requirements for these types of disclosures set out in the Privacy Rule.

This is an outline of some of the basic information that billing and practice management companies need to know to successfully navigate the Business Associate requirements of the HIPAA Privacy Rule. On April 14, 2003, the requirements for these agreements begin to kick in, and by April 14, 2004, every relevant relationship that the company has should be compliant with these requirements. As with all the HIPAA Privacy requirements, this one is do-able, and compliance efforts should be scaled to the size and needs of the organization.

If all else fails and panic sets in, remember to repeat the unofficial HIPAA mantra: *Reasonable Safeguards*. That's the ultimate requirement for protection of patient privacy, and is possible to achieve with some work and a little help from your friends. ◆

Karen Collier is Corporate Compliance Officer and Privacy Officer for Emergency Physicians Billing Services in Oklahoma City, OK. She can be reached at collierk@epbs.com.