Update on Business Partner/Associate Agreements (HIPAA on the Job)

by Bonnie S. Cassidy, MPA, FHIMSS, RHIA

If you're wondering how to interpret the proposed privacy and security rules related to HIPAA, you're not alone. The requirements of these rules—and the similarities and differences between them—are surrounded by confusion and controversy.

Having recently attended AHIMA's National Convention and the JHITA conference on HIPAA, I have realized that there are many different views and opinions on all of the proposed regulations. As you navigate through them, please keep in mind that at this time, the proposed requirements are just that-"proposed." With the exception of transactions and code sets, at press time, final regulations have not been released.

Another reminder: To enhance your understanding of the proposed rules on security and privacy, read the actual documents in the Federal Register. This is daunting, but it is a must. You can access these documents online at http://aspe.os.dhhs.gov/admnsimp.

One of the most frequently cited "gray areas" is related to the topic of business partner/associate (BP/A) and chain of trust agreements. In this article, we'll revisit this difficult issue.

Privacy vs. Security Basics

Privacy, in the context of HIPAA, addresses **the rights** of an individual regarding his or her individually identifiable health information; how to exercise those rights; the responsibilities of organizations to support an individual's rights; and the use and disclosure of that information. See Section 164.506(e) of the proposed privacy rules covering business partner agreements and contracts for more details.

Security is the means by which the **confidentiality** of information and rules for use and disclosure are implemented. Security also extends to the integrity and availability of health information and includes information that is not individually identifiable. See Section 142.308 (a)(1) for more details on the proposed security regulations covering chain of trust agreements.

A key question in sorting out HIPAA-related business partner issues is **"Is there access to protected health information (PHI)?"** If the answer is no, then you may not have issues. If yes, then you need to review and amend existing contracts or create new contracts with these entities.

When it comes to protecting "access" to PHI, we will be referring to BP/A agreements. When we think not only of access but "sharing and/or processing" of PHI, we will be referring to chain of trust agreements.[1]

What Is a Business Associate Agreement?

BP/A agreements (formerly referred to as "business partner agreements") are a requirement under the proposed **privacy rules**.[2] These agreements are required between entities that provide access to PHI.

Section 164.506(e) of the proposed privacy regulations would require covered entities to take specific steps to ensure that PHI disclosed to BP/As remains protected. The intent is for these provisions to allow customary business relationships to continue while protecting the information shared in these relationships. BP/As would not be permitted to use or disclose PHI in ways that would not be permitted of the covered entity itself.

Other than for purposes of consultation or referral for treatment, covered entities are not allowed to disclose PHI to BP/As. The relationship would include a written contract that would limit the BP/A's uses and disclosures of PHI to those permitted by the contract and would impose certain security requirements.

A covered entity would be held responsible for violations by BP/As.

Who Is a Business Partner/Associate?

According to the proposed privacy rule, a BP/A would be a person to whom the covered entity discloses PHI so that the person can carry out, assist with the performance of, or perform a function or activity for the covered entity. This would include contractors or others who receive PHI from the covered entity (or from another BP/A of the covered entity), **including lawyers, auditors, consultants, third-party administrators, healthcare clearinghouses, data processing firms, billing firms, and other covered entities. This would NOT include members of the covered entity's work force.**

In the October 2000 installment of "On The Job," it was indicated that business partner agreements are not required for the purpose of treatment, payment, and healthcare operations. **Please note that this subject continues to be controversial. Organizations should consult legal counsel in determining with whom BP/A and chain of trust agreements are needed.**

Some experts believe that covered entities will need a BP/A agreement with physicians because PHI is shared. Until final rules are released, a final determination is unknown.

Opinions on this issue vary widely. One interpretation is that a physician (a member of your medical staff) and a hospital do not need a BP/A agreement as they are both covered entities under HIPAA and the physician is working with the hospital for the purpose of treating patients.

If, however, a physician is on a committee, some experts believe a BP/A agreement is needed. On the other hand, others believe that these committees support the hospital and are included in "healthcare operations," so an agreement would not be needed.

What Are Some Examples of Business Partners/Associates?

Under the proposed regulations, **billing agents, auditors, third-party administrators, attorneys, private accreditation organizations, clearinghouses, accountants, data warehouses, and consultants** would be considered BP/As of a covered entity. Most covered entities will use one or more BP/As to assist with functions such as **claims filing, claims administration, utilization review, data storage, or analysis.** Other examples would include:

- Joint Commission surveyors at the time of survey
- consultants working on your annual financial audit
- information consultants working in the HIM department
- attorneys working with the compliance office or internal audit department

The issue has many dimensions. An entity may have business relationships with organizations that would not be considered business partners because PHI is not shared—for example, for facility management or food services. In the case where an entity provides management services to another organization, the other organization would not be a business partner because it would be receiving, not providing, a service or function.

"Incidental access" to PHI could be reason to have a BP/A agreement, as with a hospital's environmental services contract. Environmental services workers do not need access to PHI to do their job, but if they **should** have access it, the entity may want to be sure that it is protected via a BP/A agreement.

A covered entity could become a BP/A of another covered entity, such as when a health plan acts as a third-party administrator to an insurance arrangement or a self-funded employee benefit plan. In such cases, the proposed rule says that the authority of the covered entity acting as a BP/A to use and disclose PHI should be constrained to the authority that any partner or associate in the same situation would have. Thus, the authority of a covered entity acting as a BP/A to use and disclose PHI would be limited by the contract or arrangement that created the relationship.

In most cases, **healthcare clearinghouses** would fall under the definition of BP/A because they receive PHI to provide payment processing and other services to plans, providers, and their business partners. In this case, although clearinghouses would be covered entities, in many instances they would also be treated as business partners of providers or plans for whom they are performing a service.

short cuts for BP/A, CTA agreements

Proposed **privacy** rule->**access** to health information->**BP/A** agreements with individuals who are not members of the healthcare organization's work force

Proposed **security** regulations->**sharing/processing** of health information->**chain of trust** agreements[3]

What Are the Limitations on Use or Disclosure?

Use or disclosure is limited in two ways. The first is **scope of the covered entity's authority.** According to the proposed rules, when a BP/A is acting on behalf of a covered entity, its use or disclosure of PHI would be limited to the same extent as that of the covered entity for whom it is acting. For example, a business partner could not sell PHI to a financial services firm without individual authorization because the covered entity would not be permitted to do so under the proposed rules.

Similarly, a BP/A would be bound by the terms of the notice of the covered entity from which it obtains PHI. For example, if a covered entity provides notice to its subscribers that it would not engage in certain permissible disclosures of PHI, then such a limitation would apply to all of its BP/As. This approach ensures that individuals can rely on the notices that they receive from the entities to which they disclose PHI.

Use and disclosure are also limited by scope of contractual agreement with the covered entity. A contract could not grant a BP/A authority to make uses or disclosures of PHI that a covered entity would not have the authority to make. The same limitations would apply to a BP/A's subcontractors. See "Contract Specifics."

What About Agreements between Two Physicians?

When a covered entity consults with or makes a referral to another covered entity for the treatment of an individual, the rule proposes that the sharing of PHI pursuant to that consultation or referral not be subject to the contracting requirement described above.

Unlike most business partner relationships, which involve the systematic sharing of PHI under a business relationship, consultation and referrals for treatment occur informally among peers and are specific to a particular individual. Such exchanges of information for treatment also appear to be less likely to raise concerns about further impermissible use or disclosure, because providers receiving the information are unlikely to have a commercial interest in using or disclosing it.

Covered healthcare providers receiving PHI for consultation or referral purposes would still be subject to this rule and could not use or disclose such PHI for a purpose other than the purpose for which it was received (i.e., consultation or referral).

BP/As (including those that are covered entities) that have contracts with more than one entity would have no authority to combine, aggregate, or otherwise use for a single purpose PHI obtained from more than one covered entity unless doing so would be a lawful use or disclosure for each of the covered entities that supplied it.

In addition, the BP/A must be authorized through the contract or arrangement with each covered entity that supplied the information to combine or aggregate the information. For example, a BP/A of a health plan would be permitted to disclose information to another health plan for coordination of benefits purposes, if such a disclosure were authorized by the business partner's contract with the covered entity that provided the PHI.

However, a BP/A performing an audit of a group medical practice on behalf of several health plans could NOT combine PHI that it had received from each of the plans, even if the business partner's contracts with the plans attempted to allow such activity, because the plans themselves would not be permitted to exchange PHI for such a purpose. A covered entity would not be permitted to obtain PHI through a business partner that it could not otherwise obtain itself.

A BP/A generally could create a database of deidentified health information drawn from the PHI of more than one covered entity with which it does business and could use and disclose information and analyses from the database as they see fit, as long as there was no attempt to reidentify the data.

For example, the BP/A could review the utilization patterns of a group medical practice on behalf of several groups of plans by establishing a database of deidentified health information drawn from all of its contracts with covered entities and review the use patterns of all of the individuals in the database who had been treated by the medical group. The results of the analyses could be used by or distributed to any person, subject to the limitation that the data could not be identified.

What About Accountability?

Covered entities are accountable for the uses and disclosures of PHI by their BP/As. For example, a covered entity would be in violation of the proposed privacy rule if it knew or reasonably should have known of a material breach of the contract by a business partner and failed to take reasonable steps to repair the breach or terminate the contract.

A covered entity that is aware of impermissible uses and disclosures by a BP/A would be responsible for taking necessary steps to prevent further improper use or disclosures and, to the extent practicable, for mitigating any harm caused by such violations.

This could include, for example, requiring the BP/A to retrieve inappropriately disclosed information (even if the partner or associate must pay for it) as a condition of continuing to do business with it. Where a covered entity acts as a BP/A to another covered entity, the entity acting as BP/A would also be responsible for any violations of the regulation.

What Is a Chain of Trust?

Chain of trust agreements (CTAs) are required under the proposed **security standard,** but nothing in those regulations describes what provisions the CTA must include. **CTAs are required between entities that "share and process" PHI electronically.** Currently, if a provider wants to submit claims electronically to a payer, the provider and payer enter into a contract that defines how the communications will be done, when and if remittance advices will be provided electronically, how often the transmission will occur, in what format the transactions should be submitted, and so on. That contract is not currently referred to as a CTA, but it could be considered one.

The chain of trust concept of the proposed security rule extends protection to external trading partners with whom we exchange patient information electronically—e.g., a clearinghouse or payer. A physician is not typically a trading partner and would not fall under the chain of trust requirements. However, physicians are still required to comply with an organization's internal confidentiality agreements and security awareness training—as are all employees, internal staff, and external vendors.

Remember to review similar scenarios with your legal experts to be sure that you and your organization are protected and HIPAA compliant.

Notes

1. Dennis, Jill Callahan. Presentation at 2000 JHITA HIPAA conference, Chicago, IL, September 29, 2000.

2. Margret Amatayakul, FHIMSS, RHIA, announced at a pre-workshop session of the JHITA conference that this wording changed from business partner agreements to business partner/associate agreements, September 27, 2000.

3. Dennis, Jill Callahan.

Contract Specifics

In light of the ins and outs of BP/A requirements, contracts assume a great deal of importance under HIPAA. According to the proposed rule, covered entities cannot disclose PHI to BP/As unless the two have entered into a written contract that meets HIPAA requirements.

Such a contract would:

- prohibit the BP/A from further using or disclosing the PHI for any purpose other than stated in the contract
- prohibit the BP/A from further using or disclosing the PHI in a manner that would violate the requirements of this proposed rule if done by the covered entity
- require the BP/A to maintain safeguards as necessary to ensure that the PHI is not used or disclosed except as provided by the contract. For example, if the BP/A is a two-person firm, the contractual provisions regarding safeguards may focus on controlling physical access to a computer or file drawers, while a contract with a business partner with 500 employees would address use of electronic technologies to provide security of electronic and paper records
- require the BP/A to report to the covered entity any use or disclosure of the PHI not provided for in the contract
- require the BP/A to ensure that any subcontractors or agents to whom it provides PHI received from the covered entity will agree to the same restrictions and conditions
- establish how the covered entity would provide access to PHI to the subject of that information when the business partner has made any material alteration in the information
- require the BP/A to make available its internal practices, books, and records relating to the use and disclosure of PHI received from the covered entity to HHS or its agents
- establish how the entity would provide access to PHI to the subject of that information in circumstances where the BP/A holds the information and the covered entity does not
- require the BP/A to incorporate any amendments or corrections to PHI when notified by the covered entity that the information is inaccurate or incomplete
- at termination of the contract, require the business partner to return or destroy all PHI received from the covered entity that it still maintains and prohibit the partner from retaining it
- state that individuals who are the subject of the PHI disclosed are intended to be third-party beneficiaries of the contract
- authorize the covered entity to terminate the contract, if the covered entity determines that the BP/A has repeatedly violated a term required by this paragraph

Bonnie Cassidy, MPA, FHIMSS, RHIA, *is a principal with the North Highland Company, Atlanta, GA. She recently received AHIMA's Legacy Award. She can be reached at bcassidy@ north-highland.com.*

Article citation:
Cassidy, Bonnie S. "Update on Business Partner/Associate Agreements (HIPAA on the Job series)." *Journal of AHIMA* 71, no.10 (2000): 16A-D.