Understanding Chain of Trust and Business Partner Agreements (HIPAA on the Job)

by Bonnie S. Cassidy, MPA, FHIMSS, RHIA

Confused about the differences between privacy and security? You're not alone. Combine these with the jargon-laden chain of trust and business partner agreement issues, and a whole new set of questions about HIPAA implementation emerges.

Privacy, pursuant to 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.

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 health information that is not individually identifiable.

The HIPAA regulation on privacy, when it is finalized, will have important implications for an organization's HIPAA security effort. As your organization considers the implications of the privacy and security rules, anticipate key provisions such as:

- **policies, processes, and safeguards** to ensure the use of the "minimum necessary" individually identifiable health information for a given use or disclosure. This should define certain requirements for security, including access controls and increased creation and use of deidentified data
- **audit trails of disclosures** pursuant to required authorizations. For example, prior authorization is required for use or disclosure of all identifiable health information for marketing. This requirement should be built into security decisions on audit trails
- **processes for making addenda and corrections and notifying other information users.** If the process for modification and notification is going to be automated, it should be anticipated with other HIPAA requirements
- **processes and controls for enabling additional restrictions on access** to identifiable health information, which could define additional access controls and authorization processes
- **business partner requirements,** which should be considered at the same time as chain of trust partner agreements
- **training requirements** for privacy, which should be coordinated with security training[1]

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 health information 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.

Business partner agreements (BPAs) are a requirement under the **privacy regulations**. A covered entity must include three basic overriding principles in its contract with a business partner, and the proposed privacy regulations would include nine specific provisions as well. BPAs are required between entities that share protected health information-regardless of whether the sharing is done by talking, writing, copying, faxing, electronically, or some other way.

Currently, no state or federal laws require BPAs. As an example, when a consulting firm conducts an audit of a covered entity's revenue cycle, the covered entity will most likely provide the firm access to protected health information. In addition, the firm may require the covered entity to sign an engagement letter that describes the scope, approach, timing, and fees for the project/engagement. That engagement letter (also referred to as a letter of understanding or arrangement letter), however, does not include most, if any, of the provisions that are mandated under the privacy regulations. As such, an engagement letter without modifications cannot be considered a BPA.

What Is a Chain of Trust?

The chain of trust concept of the security regulations extends protection to external trading partners with whom we exchange patient information electronically. An example of a trading partner would be 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.

The proposed privacy rule (164.518 [b][2][iii]) states: "The covered entity must require members of its workforce trained as required by this section to sign, at least once every three years, a statement certifying that the person will honor all of the entity's policies and procedures required by this subpart."

What Is a BPA?

A BPA, according to the privacy regulations, extends a long list of terms to both trading partners and other vendors with whom we may not exchange information electronically, but who may have access to the information during the normal course of business or providing services. This may include software vendors, consultants, and maintenance firms. Business partner agreements are not required for the purpose of treatment, payment, and healthcare operations. Physicians, for example, would not need a business partner agreement with the hospital.

How Do the Security and Privacy Proposed Rules Differ Regarding CTAs?

There seems to be considerable overlap and some conflict between the proposed security and privacy rules regarding chain of trust and business partner agreements. The two overlap in their basic intent to protect the confidentiality of individually identifiable health information, but they also differ.

The **security rule** calls for "security measures" to be maintained at a minimal and acceptable level throughout the trading partner chain when exchanging protected health information. This means that the same level of protection measures established by the host partner shall be maintained by the receiving trading partner(s).

The **proposed privacy rule** addresses the specific "accountabilities" to which business partners must adhere. These accountabilities are required to mirror the host partner's responsibilities as defined under the proposed rule. For example, this includes rules for "disclosure" and "use" of protected information. Also, such BPAs shall contain remedies, penalties, and termination provisions, as appropriate.

The proposed rules defined under security and privacy regarding business/trading partners are important and should be assessed and implemented under the guidance of your organization's legal counsel.[2]

How Can I Tell the Difference Between CTAs and BPAs?

BPAs are very different from CTAs. BPAs must include specific provisions that are spelled out in the privacy regulations.

What probably currently exists between covered entities and their "business partners" (this, too, is a new term; no state or federal law currently defines "business partner") is a contract that defines how the two will communicate information electronically.

As such, the only thing that agreement can be called is a CTA. This may be confusing to most people as the industry has recently adopted the term "business partner" and everyone assumes that a contract with a business partner is, therefore, a

BPA. The contract may actually have nothing to do with sharing protected health information.[3]

What If I Work for a Clearinghouse?

If you work for a clearinghouse, it is obligated to meet the HIPAA security regulations. Your business partners, therefore, would also be obligated to your level/standard of data security. This should be addressed in your contract. Because this data sharing is critical to operations, the notification of disclosure to the patient would occur only upon his or her demand via the security officer or designee.

Can An Individual's Health Information Ever Be Disclosed Without Authorization?

As a general rule, covered entities would be able to use or disclose an individual's protected health information without authorization for the purposes of treatment, payment, and healthcare operations. Further, the clearinghouse's contractual relationship with its subcontractor should spell out the expectation that a certain standard of data security is required. The covered entity would not be required to provide an accounting of disclosures for treatment, payment, and healthcare operations.

Can a Patient Get an Accounting of Disclosures?

Under the proposed regulations, the patient would not be entitled to an accounting of disclosures made by a covered entity for treatment, payment, or healthcare operations (164.515[a][1]), even if he or she demanded it. This would cover most disclosures by a clearinghouse to its business partners.

How Should We Treat Affiliates?

It is advisable for any entity sharing protected health information with another entity to address that arrangement in an agreement, either a CTA (under the proposed security rule) or BPA (under the proposed privacy rule). An example would be those affiliates to whom hospitals have voluntarily released patient information (physician practices or groups like radiologists or pathologists that are either given direct access to the database or have the information transmitted to them in some fashion). Make sure the affiliates understand the limitations on the use of that information as well as the requirement that the information be kept secure.

The exact terms of that agreement will vary depending on the nature of the relationship, whether it is a provider and a business partner, a provider-to-provider transfer, where both gain access to information for treatment purposes, or provider to payer. The proposed regulations do have specific terms that should be included in provider-to-business-partner or provider-to-chain-of-trust-partner agreements.

Depending on the situation, you could take the position that pathologists and radiologists are acting as providers in the patient care continuum and would be considered providers, which for disclosures for the purposes of treatment would not require a BPA. Neither would a patient authorization for release of information or disclosure of release of information to the patient be required.

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

Final Transactions, Code Sets Rule Published

In August, the Department of Health and Human Services (HHS) published the final regulations concerning HIPAA transactions and code sets. The new standards establish standard data content and formats for submitting electronic claims and other administrative health transactions. By promoting the greater use of electronic transactions and the elimination of inefficient paper forms, the administrative simplification regulations are expected to provide a net savings to the healthcare industry of $29.9 billion over 10 years, according to an HHS press release.

Health plans, clearinghouses, and providers that transmit transactions electronically will be expected to comply with the rules within 26 months of publication of the final rule-October 2002.

HHS Secretary Donna Shalala stressed that the rule assumes that privacy protections will be in place by the time the rule takes effect. "If such protections were not in place," the press release states, " HHS will seriously consider suspending or withdrawing the transaction regulation."

The text of the final rule is available online at http://aspe.os.dhhs.gov/admnsimp/index.htm and in the August 17, 2000, *Federal Register*.

Notes

1. Koss, Shannah. "Getting Ready for HIPAA Security Requirements." Paper presented at HIMSS 2000 National Convention, Dallas, Texas, April 2000.
2. "Frequently Asked Questions." Available at the HIPAAcomply Web site, www.HIPAAcomply.com.
3. Interview with Lisa Dahm, JD, Deloitte & Touche LLP; Houston, TX, August 1, 2000.

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

Article citation:
Cassidy, Bonnie S. "Understanding Chain of Trust and Business Partner Agreements." *Journal of AHIMA* 71, no.9 (2000): 16A-C.
