# Mind Your Business Associate Access: Six Steps

Save to myBoK

*by Tori Sullivan, RHIA*

It's April 10, 2003, and a privacy officer is reviewing her policies for the imminent privacy regulations, title II of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The compliance deadline is April 13, 2003, and she is already feeling stressed about meeting the date. The organization's CIO mentions that one of their databases has been experiencing problems, and the vendor responsible for the product has been doing work on the database remotely. He says that the vendor has requested the organization send a copy of yesterday's data to its headquarters.

Once the vendor has completed its assessment, the CIO wants to be sure their data will be destroyed, not returned to the organization, and presses the privacy officer for a copy of the organization's contract with the vendor. The privacy officer realizes she never renegotiated contracts with their vendors during the HIPAA implementation process. How will the vendors handle her organization's patient health information when it is out of the organization's hands?

Many organizations have been focusing on internal compliance requirements regarding the aspects of HIPAA. Unfortunately, while the HIPAA regulations do not detail how healthcare organizations should ensure business associates are compliant while working on their databases, they are required to deal with how their business associates are going to handle their data under HIPAA regulation. This article provides six steps to maintaining compliance when business associates have access to your organization's data.

**Step 1:**
**Understand the Regulations**

Understand the HIPAA regulations and timelines that pertain to business associates and patient health information. For the purposes of this article, I will focus on two big areas involved in the regulations—privacy and security. Privacy regulations focus on managing the permitted use, disclosure, or access to protected information. Security regulations focus on safeguarding and insuring the privacy of secured information through controlling access to the information and protecting it from inappropriate disclosures and accidental or intentional destruction or loss. The privacy regulations have been finalized, however, at press time, the security regulations are still in the "proposed" status.

**Step 2:**
**Identify Business Associates**

Identify your organization's business associates. Business associates can be defined as entities that perform functions on behalf of a healthcare organization that create, receive, or have access to individually identifiable health information maintained by the healthcare organization. Typically, healthcare organizations have current contracts with business associates called business partner agreements.

These contracts will need to be reevaluated to ensure that the business partner is upholding the privacy and security regulations of HIPAA. Once the healthcare organization has defined who its business associates are, it needs to define its privacy and security expectations of its business associates in regard to HIPAA compliance.

**Step 3: Develop Requirements for Business Associates**

The proposed security rule includes four categories of requirements: administrative safeguards, physical safeguards, technical security services, and technical security mechanisms. These categories can dictate how patient health information should be accessed and utilized by the business associate.

Administrative safeguards include measures to protect data such as forming and managing security policies and procedures. They also include controlled access to patient health information and written policies and procedures to support irregular situations that could result in a security or privacy breech.

Physical safeguards are designed to protect the physical control of patient health information. Physical safeguards include media control, physical access control, and training regarding security policies and procedures. Security standards apply to the healthcare organization as well as its business associates. The technical securities and mechanisms are put in place to protect electronic data, including limiting access and creating integrity controls for private and secured information.

Because of the complexity of the renegotiation process, it may be advantageous for the organization to negotiate an amendment and renegotiate a new contract at the expiration of its current contract. Healthcare organization should be aware of any contracts that are automatically renewed each year, as they too must be renegotiated prior to April 14, 2003.

**Step 4: Evaluate and Update Business Associate Contracts**

Amendments and renewed contracts are legally binding promises between a healthcare organization and its business associates. Contracts should include a clause stating the retention, return, or destruction method for all patient health information that has been transported to the business associate.

Patient health information that was sent to the business associate should be destroyed and not returned. The method of destruction should be specified within the contract, along with proof of destruction. A termination clause should also be included in the contract, and both the business associate and the healthcare organization must sign the contract in order for it to be a legally binding agreement.

**Step 5:**
**Create Policies and Procedures**

Internal policies and procedures should be created to ensure privacy and security of health information. Healthcare organizations should have a policy and procedure for sending patient health information to business associates that includes information on the method and form of delivering the patient health information. They should also set up secured environments for business associates to access patient health information from outside the organization.

Policies and procedures should be created and implemented for business associates that will need access to the organization's network. Organizations can utilize firewalls, routers, and switches to assist with network-based filtering, as well as user IDs and passwords to assist with identification and authentication controls.

**Step 6:**
**Implement New Regulations**

Review the steps listed above and create a plan of action for each step that outlines the current status, task that need to be completed, and resources needed to complete each task, as well as realistic timelines for completion. HIPAA requirements include staff training, which should include materials outlining the policies and procedures, as well as the significance of the privacy and security regulations.

Staff members must be held accountable for violating privacy or security policies. Training should be conducted prior to April 14, 2003, and continued on an annual basis, given that regulations are subject to change over time. Policies and procedures should also be documented and updated each time they are modified and reviewed at least on an annual basis. The implementation process can be time consuming and cumbersome, which is why it is best to get started as soon as possible.

**References**

AHIMA Policy and Government Relations Team. "A Review of the 2002 Department of Health and Human Service Notice of Proposed Rule Making for The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Regulations." Available online in the FORE Library: HIM Body of Knowledge in the Communities of Practice at www.ahima.org.

Brandt, Mary. "HIPAA Security Standards: Working with Your Information Technology Vendors." AHIMA Convention Proceedings. Miami Beach, FL, October 2001.

Cassidy, Bonnie S. "Understanding the Chain of Trust and Business Partner Agreements." *Journal of AHIMA* 71, no 9 (2002): 16A-16C.

Hanks, Tom. "Compliance Issues and the Impact of HIPAA Security and Privacy Regulations." Presentation at the AHIMA Convention, Chicago, IL, September 2000.

Hjort, Beth. "Practice Brief: HIPAA Privacy and Security Training." *Journal of AHIMA* 73, no. 4 (2002): 60A-60G.

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. Federal Register 67, no. 157 (August 14, 2002). Available at www.hhs.gov/ocr/ hipaa/privrulepd.pdf.

Wagner, Lew. "Uniting Security Forces Against Risk." *Journal of AHIMA* 73, no. 6 (2002): 39-42.

***Tori Sullivan*** *(ToriS@softmed.com) is a senior consultant in professional services at SoftMed Systems, Inc.*

**Article citation**:
Sullivan, Tori. "Mind Your Business Associate Access: Six Steps." *Journal of AHIMA* 73, no.9 (2002): 92ff.