

## Why Comply with HIPAA?

By Bob Radecki

### Background

In my HIPAA article in the January issue of Health Insurance Underwriter Magazine, I described some of the changes made to HIPAA by the section of ARRA called the HITECH Act, and argued that now is a good time for insurance agents and brokers to get serious about HIPAA. As you know by now, ARRA made Business Associates, like insurance agencies, directly subject to HIPAA rules and regulations effective February 17<sup>th</sup>, 2010. Since the January article was released I have received a number of comments and questions that, for the most part, fell into two general categories.

1. Inquiries from agents and brokers who wanted to understand what they actually had to do to comply with HIPAA.
2. The other common question I received was some version of "Why should I care?"

In this article I will try to address both questions by sharing examples of common HIPAA mistakes, and by explaining what it takes to actually comply with HIPAA.

### Mistakes and Consequences

Not only large insurance companies and medical providers experience privacy and security problems. A simple search on the internet reveals example after example of violations, complaints and breaches at even the smallest of companies. Consider the following examples. The identity of the firms involved is often public but I have chosen not to identify organizations by name.

- In 2008 a sales representative of an insurance agency in the Southeast had a laptop stolen. The laptop contained the personal information of the employees of a local school district. The local press named the agency and reported that the laptop contained names, birthdates, social security numbers, and medical history information. The agency responded that the laptop was password protected but did not make it clear if the data was encrypted
- A complaint about an insurance agency was lodged on a website where individuals seek legal advice. According to the complaint an agent called the workplace of an employee's spouse to follow up about her information on the medical history section of an application. The employee's spouse was not at the office at the time, and instead of calling back, the agent asked personal medical related questions to the spouse's secretary!
- A Utah woman had her health plan enrollment information stolen which was then used by someone who had a baby. After the infant tested positive for the mother's illegal drug use, authorities confronted the Utah woman and threatened to take away her other children. The woman was forced to prove she had not had a child in years and that she had been the victim of medical identity theft.

These examples illustrate the consequences of some of the most common HIPAA shortcomings I encounter in my practice. Here are my top areas of concern regarding HIPAA compliance at insurance agencies.

#### Staff lack of understanding of the rules

The number one cause of HIPAA related mistakes is internal staff ignorance or malfeasance. Agency employees sometimes do not even understand what information is subject to HIPAA. I often hear

comments like “I don’t see detailed medical claims, so I don’t have to worry about it”. This misses the point the even health plan enrollment information is considered Protected Health Information (PHI) and is subject to HIPAA Privacy and Security rules. Just ask the woman in the example from Utah if basic plan information is important.

#### Removable electronic media - the Achilles heel of electronic security

I have worked with clients who had done a good job of implementing security policies such as network security, access controls, and physical security of company computers only to allow employees to save files on unsecure USB drives (which seem to be lost more often than an old pair of sunglasses).

#### Poor physical security and separation of access

Many agencies have a variety of employees performing different functions (i.e. employee benefits, P&C, financial consulting, general operations). HIPAA is clear that only certain employees have a right to access and use health plan related information. To comply with HIPAA a firm must implement reasonable physical safeguards to limit access to PHI to appropriate staff. Yet I often find situations where simple, inexpensive, steps to protect PHI are not employed. Consider implementing basic safeguards such as using locked file cabinets, destroying old client records no longer in use, setting up a locked file room with limited access, and physically separating the employee benefits and P&C departments.

#### Complacency

Many agencies feel that they are “under the radar” or are not likely to experience HIPAA problems. Before ignoring HIPAA you may want to speak with the small Western agency that had one of their computers, which contained detailed client records, stolen from their office. You can still find a copy of their communications to clients and the state Attorney General regarding the incident on the Internet.

### **Steps to Effective Compliance**

Effectively, compliance with HIPAA involves more than simply training your employees (although that is an important step). Compliance should also not break the bank or overly burden your staff; after all you have a business to run. Here is my attempt to describe the most important elements of an effective and comprehensive HIPAA compliance process.

#### Create “real” written HIPAA policies and procedures – and follow them.

Policies and procedures to address the multiple HIPAA requirements must be written and communicated to employees. More importantly they must accurately reflect what you actually do! That may sound pretty basic, but I often find organizations that have purchased a HIPAA manual or software and simply printed everything out, signed it, and stuck it in a three ring binder. Sure they have written policies and procedures, but what’s the point?

Recently I was retained by an agency to do a review of a client’s HIPAA privacy and security policies. The agency said the client had written policies and procedures. During the review I found policies specifically related to a physician’s treatment of their patients. Since the employer was in the food service industry, and did not employ any medical providers, it was obvious that no one had ever even read their policies!

#### Perform a HIPAA security assessment

An often overlooked, yet required step to HIPAA compliance is to perform (and document) a security assessment. §164.308 of HIPAA requires an entity to “*conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the...entity.*”

#### Pay attention to the HIPAA Security Rules

Many organizations made an honest attempt to comply with the HIPAA Privacy Rules, then for some reason, decided to ignore the separate (and I would argue just as important) HIPAA Security Rules. The HIPAA Security Rules contain 20 separate “standards” that an entity must address. The standards deal with things like workstation security, facility access control and contingency planning. The good news is that organizations often find they are able to leverage existing company security policies and procedures to meet many of these standards. If you are already doing a good job related to security in general, HIPAA will not require you to reinvent the wheel, but you will need to make sure all of the standards are addressed and create policies for those that you do not already have covered.

#### Extend compliance obligations to vendors and subcontractors

Just as a health plan must enter into a Business Associate Agreement with you, HIPAA requires a Business Associate to extend requirements designed to protect the privacy and security of PHI to its vendors and subcontractors who use or have access to PHI. You need to add language very similar to that contained in a Business Associate Agreement to your contracts with some of your vendors.

#### Train Employees and Implement Sanctions for Violations

Employees must be trained on HIPAA in general, and on your organization’s specific policies and procedures. HIPAA also requires an organization to apply sanctions to employees who violate HIPAA or your policies. §164.530(e) of HIPAA states that “...an entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the ...entity or the requirements of (HIPAA)”

#### **Summary**

As I was completing this article I received a phone call from a large agency in Rhode Island. While discussing why HIPAA compliance was important to their firm, a Principal of the agency made a straightforward statement. He simply said “It’s the right thing to do”.

#### **About The Author**

Bob Radecki is currently a Principal at the HR consulting firm of W.J. Flynn and Associates, LLC and manages the HIPAA compliance organization KnowHIPAA.com. Bob has over 25 years experience helping brokers and employers deal with difficult compliance issues. Bob founded and, for over 10 years, served as President of A.E. Roberts Company, a nationally recognized compliance consulting and training firm. Bob was also the principal HIPAA consultant to a number of health insurance companies and has been the featured speaker at many industry events. Bob can be reached at [bob.radecki@wjflynnandassociates.com](mailto:bob.radecki@wjflynnandassociates.com). For more information call 612-581-6281 or go to [www.KnowHIPAA.com](http://www.KnowHIPAA.com).