HCCA

HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

Volume Eleven
Number Eleven
November 2009
Published Monthly

Feature Focus:

Managing risks when implementing the new EHR disclosure accounting requirements of ARRA

PAGE 28

Meet

Brenda S. Tunstill, Corporate Compliance Officer, Mercy/St. John's Health System

PAGE 14

Earn CEU Credit

WWW.HCCA-INFO.ORG/QUIZ, SEE PAGE 48

EMPLOYEE THEFT RISES DURING ECONOMIC DOWNTURN

PAGE 45

Letter from the CEO

When is the Risk department a risk to compliance?

Not all risk professionals understand compliance.

Before I get the e-mails and the phone calls, I want to be perfectly clear that the problem I am pointing out does not apply to all risk programs. There are compliance risk programs run by effective risk managers who understand compliance. The examples I give and the statements I make are related only to the risk programs that claim to be helping compliance and, in fact, are not. To try to make this fair and clearly demonstrate that this is not a rare problem, I Googled "Sample Risk Assessments" and used the first two sample risk documents that came up on my screen. The point of this article is that all risk assessments are not created equal. Not all risk assessments are effective for compliance purposes. When someone who has years of risk management background says, "I can handle the compliance risk assessment," you just might want to think twice.

Before I get started, I want to share an analogy. Twelve years ago, as compliance was getting started in a big way, I told a department head from Audit that we needed to do some compliance work. He said we have always been doing compliance. I was surprised and asked what he had been doing. He said we did audits to see if vendors were double billing the organization. He said he had done an audit to see if people were cheating on their time cards. This has been an age-old problem for compliance. This guy was competent and very nice, but was clueless about what compliance was. He did not even understand that compliance programs, as defined by the US Sentencing Guidelines, looked for harm the organization was causing to others, not looking for what harm others were causing to the organization. The Risk department is now getting into compliance like Audit did years ago. Risk is having some of the same challenges that Audit did when they first started. These are hard working and very bright people; however, some are a little confused about what compliance is all about. The problem is that because they understand risk, they come charging into the room (our profession) to tell us how to do it. With your help, Risk will make great strides over the next few years, just as Audit did.

The following is the first risk assessment sample document that come up on Google. The first thing listed at the top of the document was the statement of the risk assessment's purpose, which I have included below:

> The purpose of the risk assessment was to identify threats and vulnerabilities related to the Department of Motor Vehicles – Motor Vehicle Registration Online System ("MVROS"). (See http://www.msisac.org/webcast/08_04/info/detailed_report.pdf)

This risk assessment has nothing to do with compliance as defined by the US Sentencing Commission. Many risk assessments have nothing to do with compliance. Risk managers for years have been trained to focus on risks to the organization. They are often not focused on what other organization's rules their organization might have been breaking. Any risk assessment might have merit, but few have any relation to an effective compliance program. The problem is that Risk departments insist on having control. Some even suggest they should control Compliance or that Compliance should be a subset of Risk. Compliance risk assessments, as defined by the US Sentencing Guidelines, are solely focused on what rules your organization has been breaking. People wonder why organizations are still having trouble with implementing effective compliance programs. Risk might be a good place to look.

The second sample risk assessment that came up on Google follows. I have included part of their purpose statement:

> This is a sample risk assessment checklist that can be used as a tool to analyze vulnerabilities in your data system. (See http://media.umassp.edu/massedu/policy/append1.pdf)

At least this risk assessment has some elements of compliance to it. However, it demonstrates another problem of the traditional risk assessments. They get lost in the minutia. This risk assessment has over 300 items. I gave up counting with several pages to go. A colleague of mine (Greg Triguba) calls this "Trying to boil the world." Remember, this is the second sample I came across. I haven't stacked the deck by looking for examples that prove my point. These things are everywhere. I don't think this is a coincidence. If a trained compliance professional were to spend this much time on this one risk, the building would be on fire and they wouldn't know it. This 300-plus line item

Continued on page 48

risk assessment just covers one of hundreds of organizational risks. Furthermore, the few real compliance risks that this covers have little chance of getting proper recognition, because this risk manager is checking to see if there are steam pipes below their computers. How can you possibly find a real compliance problem in this maze?

What concerns me is that many of these people want control of compliance. Some risk professionals can not overcome their principle mission, which is to protect the organization from others. They have an important job, but it is not focused on compliance. Even if they did focus on real compliance issues, they do not have the authority, accountability, or responsibility to enforce, discipline, and implement corrective action, as described by the US Sentencing Guidelines. Many are over-engineering this over-engineered concept. Now there are Enterprise-wide Risk Assessments and Governance Risk and Compliance. Every year, someone comes up with another management program-of-the-month in the area of risk. There are slick PowerPoints, lots of arm waving, and meetings. And I mean tons of meetings. There are lists, documents, spreadsheets, Gantt charts, flow charts, and more meetings. People who are committing fraud walk by the Risk War Room, glance over their shoulders, and just smile. (OK, I admit that was facetious, but this really frustrates me.)

The most effective compliance professionals I see don't fall for the concept of "boiling the world." They don't fall for the endless requests for risk assessments that focus on what harm others are doing to the organization. They get out of the micro-compliance risk assessment world and into the macro-compliance risk assessment world. They find the major compliance risks common to their industry and look into them. If they feel that the department that is primarily responsible for that risk has a handle on the potential problem, the potential problem moves lower on the risk list. They focus on departments that have not demonstrated the proper skill in dealing with compliance issues. Effective compliance professionals don't spend months and months on this. They spend more time acting than studying. They talk to people in the organization who know where their problems are and they follow up. They network with their colleagues around the country for ideas on what risks they should be looking into. They attend conferences and read articles that point to common and significant risks in their industry. Most of all, they avoid spending endless hours developing enormous lists and getting lost in the details. They don't just point to problems; they provide corrective action, discipline, and enforcement. While they are putting to bed a significant compliance issue, their old school peers are in another meeting down the hall, arguing whether or not item number 273 in the risk assessment is more or less important than risk number 272. ■

Be Sure to Get Your CHC CEUs

Articles related to the quiz in this issue of **Compliance Today**:

- **HIPAA breach notification requirments: Ensuring compliance**— By Janice A. Anderson, Thomas P. O'Donnell, and Rebecca L. Frigy, page 4
- **Steering clear of regulatory icebergs by using data analytics** — By Griffin Jacobsen, page 34
- **Employee theft rises during economic downturn** — By Denise McClure, page 45

To obtain one CEU per quiz, go to **www.hcca-info.org/quiz** and select a quiz. Fill in your contact information, read the articles, and take the quiz online. Or, print and fax the completed form to Liz Hergert at 952/988-0146, or mail it to Liz's attention at HCCA, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Questions? Please call Liz Hergert at 888/580-8373.

Compliance Today readers taking the CEU quiz have ONE YEAR from the published date of the CEU article to submit their completed quiz.