HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

Volume Thirteen
Number Eight
August 2011
Published Monthly

Meet

Catherine Wakefield
Vice President Corporate Compliance and Internal Audit, MultiCare Health System

PAGE 14

Earn CEU Credit

WWW.HCCA-INFO.ORG/QUIZ—SEE PAGE 66

Feature Focus:

Compliance officers beware! Feds targeting executives for prosecution and exclusion

PAGE 30

Managing conflict in the hospital: A Joint Commission requirement

PAGE 9

Top compliance and legal risks for health care in 2011, Part 1

By Steve McGraw

Editor's note: Steve McGraw is President and CEO of Compliance 360 in Alpharetta, Georgia. Steve may be contacted by e-mail at Steve.McGraw@compliance360.com.

For this two-part article, Steve conducted interviews with five attorneys from leading health care law firms to examine the most pressing compliance and legal challenges and offer their insights for mitigating the risks.

The attorneys who participated in interviews for this first part of the article included: Anna Grizzle of Bass Berry & Sims, (agrizzle@bassberry.com) on the topic of false claims risks, including self-disclosures and fraud-specific audits.

Frank Sheeder of Jones Day, (fesheeder@JonesDay.com) on the topic of adapting to the changing landscape of government initiatives.

Perhaps no other industry faces the legal and regulatory challenges as those present in health care today. Not only is there a high bar for legal risk, but these risks also have more volatility than those in other industries. With the recent passage of the Patient Protection and Affordable Care Act (PPACA), as well as the Fraud Enforcement and Recovery Act of 2009 (FERA), the bar is raised even further. And, at the state level, there is yet another layer of expanding regulatory requirements and enforcements to contend with.

To better help health care compliance and legal professionals understand these changes and take proactive steps in preparation, Compliance 360 has collaborated with Anna Grizzle and Frank Sheeder, attorneys from two of the leading health care law firms, to examine the most pressing compliance and legal challenges and to offer their insights for mitigating the risks.

False claims risks including self-disclosures and fraud-specific audits

SM: Anna, the fraud and abuse enforcement landscape has changed dramatically with the passage of FERA, the American Recovery and Reinvestment Act (ARRA), and PPACA. What do you see as the key risks facing health care provider organizations and their executives?

AG: The combination of increased enforcement and increasing resources devoted to combating fraud poses an overall risk to providers. These risks now begin at enrollment. CMS is moving from a "pay-and-chase" model to a more proactive fraud prevention model, starting with enrollment. Effective on March 25, 2011, we now have enhanced screening standards based on provider classifications.

Providers are classified as limited, moderate, or high risk. Providers in the moderate and high risk categories will face increased scrutiny during enrollment. For instance, an organization such as a clinical lab is classified in the moderate risk category. The provider will be subject to an on-site visit from CMS representatives before the enrollment application can be approved. Providers in the high risk category, such as home health agencies and DMEPOS suppliers, will be subject to the on-site visits as well as criminal background checks and fingerprinting of all investors that hold a 5% or greater interest, before the organization can be enrolled in the Medicare program.

Looking beyond enrollment, the new 60-day requirement for providers to return overpayments creates new risks. If a provider fails to return overpayments within 60 days of discovery, the retained overpayments can be classified as false claims under the False Claims Act (FCA).

Continued on page 22

 ...continued from page 21

However, there is a lack of guidance on how to measure the 60 days, which means providers face significant uncertainty as they seek to mitigate the risk of FCA actions. When does the 60-day clock start running? Is it when the provider first becomes aware that there may be an overpayment, or is it after the provider has confirmed an overpayment occurred and completed a financial analysis to determine the amount? Even for seemingly simple scenarios, 60 days is a very short time for gathering information, conducting an investigation, and reaching a conclusion. Until more clarity is provided, providers should be very proactive in their efforts to identify vulnerabilities and move quickly when correcting problems and reporting overpayments.

Another significant risk for providers is the less stringent burden of proof borne by the government when imposing payment suspensions. CMS can now impose a payment suspension pending the investigation of a "credible allegation of fraud" which can come from almost any source, as long as it has "an indicia of reliability." These sources include fraud hotline complaints, claims data mining, patterns identified through provider audits, civil false claims cases, and law enforcement investigations. Unfortunately, "indicia of reliability" is not clearly defined, but will be considered on a case-by-case basis. The effect of a payment suspension can be severe, because it can be imposed for 180 days and possibly extended for longer periods of time. This situation could create a significant issue—without payments from Medicare and Medicaid for 180 days, many providers could be forced to cease operations.

In addition to these changes, providers also continue to face a significant increase in the number of contractor audits, such as the RACs, ZPICs, and MICs. These programs continue to expand and will further subject providers to increased audit and enforcement activity.

These examples show that the heightened enforcement environment has created numerous increased risks for provider organizations as well as their individual executives.

SM: The new Stark self-referral disclosure protocol seems like it can offer some relief to these new risks, but it may also create some interesting new challenges as well. What advice would you offer to providers relative to proactive disclosures?

AG: The Stark self-disclosure protocol should provide welcome relief to providers who were struggling with disclosure decisions prior to the protocol being implemented. Because the Stark regulations are highly technical and complex, the disclosure process is also very complex. It is important to conduct a thorough analysis to determine if a Stark violation has in fact occurred. I have seen cases where a provider assumed a Stark violation had occurred, but upon further analysis, we have determined that it had not. If a Stark violation is confirmed, the provider should carefully determine which method is best for disclosure. For instance, if there is the potential for violations of other laws, such as the Anti-kickback Statute, it may be best for the provider to disclose under the OIG self-disclosure protocol instead of the Stark self-disclosure protocol. All of this can take significant time to complete. Providers must act quickly because of the new requirement to return overpayments within 60 days of identifying the overpayment. Because of the complexities involved in performing this analysis and the limited time available in which to make the determination, providers should not try to handle the disclosure alone. Providers should seek the advice of experienced regulatory counsel as soon as they become aware of a potential disclosure issue.

SM: With regard to ZPIC and Medicaid Fraud Control Unit (MFCU) audits, do you anticipate an uptick in 2011 as a result of the increased focus on fraud?

AG: Yes, absolutely. One of CMS' objectives for transitioning

from the Program Safeguard (PSC) program to the Zone Program Integrity Contractor (ZPIC) was to encourage more proactive fraud investigations. For the most part, the PSCs conducted very few proactive investigations. Where the ZPICs are up and running, we are seeing an increase in both post-payment investigations as well as pre-payment reviews. ZPICs are also imposing payment suspensions while they conduct their fraud investigations.

Providers must prepare for ZPIC investigations. Providers should know which ZPIC is assigned to their region and have a plan of action ready when the ZPIC comes calling. Some providers have been treating ZPIC audits like RAC audits, and this is a big mistake. The RACs are looking for overpayments, but the ZPICs are charged with looking for fraud. ZPICs conduct their fraud investigations and often share the results with law enforcement. These referrals are leading to FCA cases and even criminal prosecutions against providers.

Similarly, providers also need to be prepared with a plan of action if the MFCUs show up. The MFCUs have been around for quite some time. With an increased focus on Medicaid program integrity, during enrollment as well as MIC audits and the upcoming Medicaid RAC audits, we should expect to see increased referrals to the MFCUs. Obviously, if more contractors are reviewing Medicaid claims, we will see an increase in referrals to and prosecutions by MFCUs.

Adapting to the changing landscape of government initiatives

SM: Frank, can you describe what you are currently seeing as key government initiatives?

FS: Right now Steve, I believe there are five key government initiatives that are generating significant compliance and legal risks for providers. These are:

1. The government's emphasis on achieving high return on investment (ROI) for its enforcement dollars.
2. Individual accountability for organizational compliance issues.
3. Increased risks created by "data prospecting," as contrasted with "data mining".
4. Scrutiny of chief compliance officer reporting relationships.
5. Expanding focus on physician/hospital relationships.

SM: Let's explore each of these in a little more detail. Can you start by explaining what you mean by high ROI and expand on your concerns?

FS: If we look at some of the reports provided to Congress from the Health Care Fraud Prevention and Enforcement Action Team (HEAT) program, which is a joint venture between HHS and the Department of Justice (DOJ) focused on combating fraud, we see that they are measuring and reporting the ROI. Historically, the government has reported a return of $4.90 for every dollar invested in combating health care fraud, waste, and abuse. During the last three years, however, the return has increased to $6.80 for every dollar invested. This increase should become a concern for health care providers because HHS and DOJ will be expected to at least maintain this rate of return, or it will risk being viewed as not being aggressive enough in combating health care fraud.

Now, with the passage of the Affordable Care Act and the Administration's current budget proposal, we see additional dollars being used to boost anti-fraud initiatives in health care. Motivated by a need to help fund health care reform, the aggressive stance on fighting fraud is very likely to swell. And, regardless of the political debates on health care reform, efforts to combat fraud are receiving bipartisan support. These efforts are not going to diminish.

SM: Let's discuss the increased focus on individual accountability by HHS-OIG.

FS: Historically, when organizations have had instances of non-compliance, individuals who

Continued on page 24

 ...continued from page 23

own them or are associated with them have not been prosecuted. The organizations may pay fines or be excluded from participation in Medicare, but individuals are often unscathed. Regulations have been proposed that bolster the ability of OIG to exclude individuals and, recently, the Inspector General stated that his office intends to hold more individuals accountable for the misdeeds of their organizations. Basically, when reform is not effective, the enforcers step in. This should be seen as the impetus for compliance officers to redouble their efforts.

SM: You mentioned that there's a difference between data mining and data prospecting. Most of us are familiar with the concept of data mining. Can you explain data prospecting and why providers should be concerned about this approach?

FS: There's a significant, fundamental difference between mining and prospecting. When you go mining, you have already used an indicator of some kind that lets you know where to dig. Prospecting, on the other hand, is the process of figuring out where to dig. The government is in prospecting mode right now. They're not saying that Hospital XYZ has a problem and let's figure out the extent and the cause. Rather, they are looking at data in aggregate to determine which hospitals have a suspected issue. The objective is to use the data to bring false claims allegations on a much broader scale.

SM: Frank, can you cite some examples of this data prospecting approach?

FS: The recent infusion therapy, blood transfusion, and lithotripsy anti-kickback cases are good examples of this. Through data prospecting, the government proactively analyzed data to identify issues, rather than react to an indicator, such as a whistle blower allegation. You should note that this approach is also driven by the need to return a high ROI on the dollars approved to fund anti-fraud initiatives.

So, with the government assiduously prospecting for outliers, hospitals should be doing the same by benchmarking their own data with that of their peers. They need to find and correct issues before the government analyzes their data and comes to the conclusion that there may have been false claims. Fortunately, most providers should be able to do this with their existing systems, but they simply have not done so.

SM: Let's talk for a moment about the focus on the reporting structure for chief compliance officers (CCOs). Guidelines in this area have been in place for years. What do you see that's different now?

FS: We are still seeing situations in which the CCO reports to the general counsel or in some cases, a single person is serving in both of these roles. OIG has long had a strong aversion to these approaches, and it recently reiterated its concerns. In light of this, at a minimum, the CCO should have a direct conduit to the board of directors or a committee of the board. Of course, the Compliance community has been addressing this issue for years, and it supports models that have an empowered and independent compliance officer. While separating the roles of general counsel and CCO may be very difficult for some organizations, separating the roles has been a strong and recurring theme that can reduce risks in a number of ways.

SM: Let's discuss the fifth of your key government initiatives—the expanding focus of OIG on physician/hospital relationships.

FS: There are a number of current investigations with implications of Stark and anti-kickback violations related to physician/hospital relationships. I anticipate that this will be a continued area of focus in the coming year. Looking ahead, I also see an interesting dilemma. Health care reform emphasizes the creation and expansion of models such as Accountable Care Organizations (ACOs) that foster collaboration for improved patient outcomes. However, we haven't seen any corresponding relief from the

Stark and anti-kickback provisions. I think it may be difficult to achieve the ground-breaking objectives of health care reform and ACOs, if we don't first remove some of the inherent risks of collaboration for providers. ■

Next month, in Part 2, Mr. McGraw interviews Sara Kay Wheeler of King & Spalding on the topic of increasing and expanding revenue recovery audits, such as RAC for Medicaid; Lisa Murtha of SNR Denton on the increasing need to demonstrate the effectiveness of compliance programs; and Lisa Ohrin of Katten Muchin Rosenman on the topic of lessons learned from recent enforcement actions and whistleblower lawsuits.