Q: Who is HCCA’s 8,500th member?

A: Mark F. Leep, MA, JD, MBA, CIP
Director, IRB and Research Compliance & Education Manager, Bon Secours Richmond Health System

See page 20

---

27
OIG’s updated Provider Self-Disclosure Protocol: Sampling and overpayment extrapolation
Cornelia M. Dorfschmid

33
Should readmissions be on a compliance officer’s radar?
Myla Reizen

37
Dealing with an even more aggressive year of enforcement
Brian G. Flood

41
Sixth Circuit Court of Appeals limits the reach of the False Claims Act
Gabriel Imperato and Shachi Mankodi
Putting “effective” into your compliance program: Implementation is more than a word

How many times have you heard about an “effective” compliance program? The word effective is defined as “adequate to accomplish a purpose; producing the intended or expected result.” It seems to be all we talk about, but it turns out there are still gaps between what we think will suffice and what we really need to implement in order to mitigate the organization’s risk.

Case in point: It was a typical litigation support project. We reviewed the compliance program policies and documentation as well as a sample of claims to find out what had gone wrong. The compliance program was neatly placed into the employee handbook. It had most of the elements we look for, including a section on audit and monitoring. According to the program, the compliance officer was going to audit billing and contracts on a quarterly basis. Nice, but where is the documentation showing the audits were performed? And if they were auditing the processes as outlined in the program, why are they in trouble?

Implementing effectiveness

The word implement is defined as “to put into effect according to or by means of a definite plan or procedure.” We have all heard the old adage that it’s better not to have a policy at all than
to have one and not follow it. The same is true with a compliance program. It might be more apparent if we structured the policies to be what they truly are—a promise of action. Each policy might say something like “By writing this policy, we promise we will comply with applicable Federal and State regulations regarding…” They might be more meaningful if they were seen as a commitment rather than merely as a document expected to be found in our arsenal. People might be more inclined to audit claims, repay credit balances, or monitor for excluded parties if the policies were written like a legal promise and if the people writing them realized they could be held liable. But policies are not, and it’s much easier to write a policy than to implement it on an ongoing basis. Implementation requires a watchdog, so to speak, to have oversight of the training and timeliness of the auditing and monitoring.

As Michael Volkov wrote in one of his Corruption, Crime and Compliance blogs,¹ the Justice Department has made it clear they have no patience for a “paper” compliance program. He wrote, “Many companies have implemented the “paper” framework for an effective compliance program. The policies are written and adopted by the company. What is missing is perhaps the most important element—implementation.”

The Federal Sentencing Guidelines are also clear: “To have an effective program to prevent and detect violations of law... an organization shall … promote an organizational culture that encourages a commitment to compliance with the law.”²

The Responsible Corporate Officer Doctrine

In order to promote an organizational culture, it takes more than paper. And now there is a resurgence of The Responsible Corporate Officer Doctrine (RCOD), which states that individuals who have an ownership or controlling interest in a sanctioned entity may be excluded if they knew or should have known of the conduct that led to sanctions, whereas officers and managing employees (which includes a general manager, business manager, administrator, or director) may be excluded based solely on their position within the entity. Thus, there is no knowledge element with respect to officers and managing employees. The concept of the RCOD arose from a pair of U.S. Supreme Court cases that held corporate officers personally liable for their corporation’s violations of the Federal Food, Drug and Cosmetic Act. In those cases, the U.S. Supreme Court found that corporate officials could have a duty to seek out and fix violations when they occur, as well as a duty to prevent violations from occurring in the first place.³

Law School in a Box

- This doctrine is an exception to the usual requirements for criminal prosecution. Ordinarily, criminal law requires a defendant to have committed a criminal act (actus reus), and to have done so with criminal intent (mens rea).

- The RCOD imposes strict liability on corporate officers, based entirely on their position within the company. With strict liability, intent is not a factor and there is generally no defense for the act. A corporate officer can be held criminally liable for a low-level employee’s criminal activity, even if the officer did not participate in or know anything about the criminal activity.

With the enactment of Section 1128(b)(8) and (b)(15) of the Social Security Act (SSA), the Office of Inspector General (OIG) now has “discretionary permissive exclusion authority.” Permissive authority means the Secretary
of Health and Human Services may exclude individuals from participating in federal healthcare programs, even if not initially convicted or excluded, and that OIG’s exercise of this discretion is not subject to administrative or judicial review.

On October 20, 2010, the OIG released guidance regarding what factors it will consider when determining whether to implement its “permissive exclusionary authority.” OIG has not yet applied its permissive exclusion authority to hospitals and health systems; however, in his keynote address at HCCA’s annual Compliance Institute in Dallas in 2010, Inspector General Daniel R. Levinson highlighted the RCOD and proclaimed that “the OIG is focused on holding responsible corporate officials accountable for healthcare fraud.” And although not directly related to the RCOD, OIG has recently excluded the chairman of a nursing home chain due to his responsibility for the provision of substandard care to residents at various facilities. Although attorneys seem to debate whether or not the RCOD will be used to prosecute healthcare executives and those in management positions, it seems prudent to prepare for that potential.

Inspector General Levinson also stated: “It is critical that boards and management make compliance with professionally recognized standards of care a priority at all levels of their organizations.” In other words, develop an effective compliance program and an organizational culture of compliance.

Because there is almost no defense to the RCOD other than that the individual was “powerless to prevent or correct the violation,” the best way to protect yourself from RCOD liability and other government imposed sanctions is to implement an effective and comprehensive compliance program. In the light of the “dangers” associated with the RCOD, we have an opportunity.

According to compliance guidance from the OIG, at a minimum, an effective compliance program should include the seven elements given in the Federal Sentencing Guidelines and must filter throughout the organization. There are no hard and fast rules, because every organization is different. Compliance programs vary, because duties may not be allocated the same way in different organizations, and organizational size and politics can change the way processes are implemented. But beyond the structural differences we may have, there are sometimes barriers to implementing an effective compliance program.

The first barrier often encountered is how to assess risks. Another seems to be applying what is learned to “doable” steps. In the litigation support example given above, the very basic paper structure was there, but it wasn’t implemented. There was no documentation of a risk assessment and the audits listed were not performed. Some audits were performed, but they did not target the risks associated with federal and state regulations, and there was no documentation to prove that the errors found were corrected.

The assessment
The first step in an assessment is to know what regulations apply to your organization. This becomes much easier when you break it down by department. Each department head should understand what regulations apply
to their area and then develop policies that
direct the employees on compliance with those
regulations. Implementation of the policies is
two-fold: training on the policies and incorpo-
rating monitoring to ensure compliance with
the regulations. The compliance officer’s duty
is to help guide them through this process,
if needed, and to make the department head
aware of other risks (e.g., whether or not there
is an OIG focus in the area, what government
contractor audits may include the area), to help
structure an effective monitoring program
that will detect non-compliance with the regu-
lations, and to have oversight of the error rates
associated with the monitoring process.

Another tool used
in the assessment
includes interviews
with key personnel
in the departments
to assess compliance
with the policies and
procedures. This
will give the com-
pliance officer the
opportunity to have
conversations that
may not otherwise take place, learn about
issues that have not been reported, assess the
overall needs of the department and, perhaps,
target education or probe audits.

Prioritizing risks
Once the assessments are complete, the com-
pliance officer can discuss the assessments
with the appropriate committees to determine
which departments are an OIG focus; need
additional resources in the form of oversight,
education, or audits; and other relevant issues.
Other organizational risks may include cur-
rent investigations, new regulations, and
issues that have become newsworthy and may
apply to the organization. Whether you rank
them using colors or numbers, it usually is
most beneficial to allocate them to a quarterly
time slot by using a tool that allows you to
track the progress and to easily convert to a
dashboard for reporting purposes. It doesn’t
have to be complicated or fancy.

Auditing and monitoring
The choice of monitoring or auditing is gener-
ally a decision based on the risk associated
with the specific process. For instance, if it
is a low-risk process that appears to be on
target and almost no error rate reported by the
department head, then continued monitoring
may suffice. However, if it is a process that
appears to hold a significant risk for the organ-
ization (due to the OIG, RAC, or other
government contracted auditor focus),
then the appropri-
ate committee may
decide to elevate the
monitoring to an
audit. The audit may
be performed by an
objective third party
within the organi-
zation who has the expertise to perform the
audit or they may elect to outsource to a con-
sulting firm that has the expertise. If the risk
appears to be significant, the organization may
decide to have the outside auditors engaged by
legal counsel under privilege.

Using an outside auditor allows the organi-
ization the ability to shadow audit in order
to learn how to audit/monitor with greater
proficiency. It’s a chance to turn a danger into
an opportunity. In fact, if there are enough
resources, it would be wise to shadow audit any
audit that is performed by another entity (e.g.,
RAC, ZPIC, etc.) It allows the organization to
know what errors may be found before they get
notice from the outside auditor, and it helps to
gain added education and expertise in the area.
Corrective actions
We all know we have an obligation to repay anything we have determined is not owed to us. Call it an overpayment or credit balance, once it has been identified, we have 60 days to repay. The clarification around the word “identified” is still not given and appears to be a slippery slope, but most people are comfortable returning money that has a dollar amount associated with the error; that is not arguable. The Centers for Medicare & Medicaid Services (CMS) has indicated that when a Medicare provider or supplier “performs an internal audit and discovers that overpayments exist,” an overpayment has been identified, triggering the obligation to report and return the overpayment within 60 days.5

At the very least, once repayment is made, the False Claims Act (FCA) requires the organization to take reasonable actions to prevent recurrence of improper claims of the same type identified in the self-audit. These reasonable actions may include process revisions, internal controls, education, and follow-up audits or monitoring activities—all of which must be documented.

Other questions that come into play are business/legal decisions regarding whether or not to pay what is owed and move forward or to look back. It has been stated often that not looking back may leave an organization open to potential qui tam lawsuits and FCA violations.

Conclusion
The process of implementing an effective compliance program is not a quick one. It includes much more than mere documents to fill a binder or space on the company intranet. An effective compliance program should be a living, breathing program. It is never finished and requires constant attention to detail. As a compliance officer, you may feel you are carrying a heavy load with a large variety of issues, and that ensuring the effectiveness of the program is just adding to that load. However, as we have seen in past judgments, an effective compliance program can help protect an organization and its officers from sanctions.6

3. For more on the RCOD, see Tom Herrmann’s article, “The New OIG Responsible Corporate Officer Doctrine.” Available at http://www.compliance.com/articles/the-new-oig-responsible-corporate-officer-doctrine/