The role of internal investigations and self-disclosure in effective compliance programs

By Matt Weber and Armin Sarabi

Editor’s note: Matt Weber is a partner in the White Collar and Health Care Industry groups in the Denver office of Holland & Hart LLP. Matt may be reached at 303/295-8565 or by e-mail at mweber@hollandhart.com.

Armin Sarabi is a student of law at the University of Denver, Sturm College of Law. Armin may be reached by e-mail at asarabi@du.edu.

The Department of Health and Human Services Office of Inspector General (OIG) recovered a reported $2.2 billion from enforcement actions in the first half of fiscal year 2008.1 During that period, OIG brought 293 criminal actions, 142 civil actions, and excluded nearly 1,300 individuals and entities for engaging in fraud or abuse in connection with federal health care programs. This recent flood of enforcement actions aimed at health care providers serves as a reminder of the severe consequences that can result from non-compliance. Compliance officers can help protect their organizations by being aware of the trigger points for fraud and abuse investigations, developing and implementing preventative measures to minimize potential exposure, initiating self-assessments, and considering disclosure of serious allegations.

Awareness, policies, and procedures

For health care providers (both entities and individuals) to minimize their exposure, they must have a good grasp of the types of activities that may trigger an investigation. Referrals and claim submissions are two primary areas of compliance enforcement. Referral issues often arise where a financial relationship exists between a health care entity and a physician who can refer patients to the entity. Enforcement officials often probe into the nature of such relationships and scrutinize practices related to office or equipment leases, medical director positions, gifts, and administrative services provided to the physician. Just about any tangible benefit exchanged between the entity and the physician may be subject to the federal fraud and abuse laws.

Inaccurate claims submissions can arise from causes ranging from truly fraudulent activity to inadvertent human or systems error. Although specific billing and coding problems vary, some of the more common ones include upcoding (coding for a more expensive procedure than warranted), unbundling (billing separately for services that should be billed as a single service), and improperly recording or rounding off time measurements for services performed.

Effective compliance plans minimize fraud and abuse risk. A compliance plan should provide a road-map to the provider’s compliance infrastructure. However, simply having a compliance plan is not enough. The elements of the plan should be explained to all relevant employees, supervisors, directors, and others through a Code of Conduct guide, compliance...
Implementing a compliance plan and policies can help safeguard providers from liability. There are, however, risks during the implementation phase. One risk is that the materials will be written in a way that sets the bar even higher than required by law. For that reason, plans and policies should be carefully crafted to avoid setting absolute or unrealistic standards. If goals are merely aspirational, they should be carefully stated in those terms. Similarly, providers should take care to not adopt policies that create too many audit points, because it may become impractical to demonstrate full compliance. Having a detailed set of procedures that are not implemented serves no useful purpose, and may undermine the provider’s credibility during a governmental investigation. It may be helpful to seek the advice of an attorney or consultant to help reduce these risks.

Self-assessment and disclosure

Despite its best efforts, a provider may find itself in the midst of a serious compliance investigation. When that happens, the provider should take the following steps with the assistance of counsel:
1. Determine the scope of the allegations;
2. Take timely action to preserve all potentially relevant documents (whether in electronic or hard copy form) and collect any appropriate information;
3. Conduct a thorough and complete investigation to gain an accurate understanding of the facts and potential penalties;
4. Take remedial measures; and
5. Audit to verify the effectiveness of the remedial measures.

These steps may overlap both in time and in substance, but each of these elements should be addressed.

It is often essential to involve counsel in self-assessments. Counsel can help ensure that proper protocols are observed to safeguard the confidentiality and independence of the investigation. Counsel can also provide valuable insight to providers when making the complex types of judgment calls that are inherent in self-disclosure decisions.

Determine the scope of the allegations

Initial allegations or governmental inquiries are often vague and far too general to offer any real insight to the scope of the problem. Nevertheless, it is always in the provider’s interest to gain an early understanding of the issue so it can get ahead of the government’s investigation, evaluate the strength of its position, and make the best case possible to the government, given the facts.

Proactive intervention can help shed light on the scope of the problem, whether the investigation is prompted by a governmental inquiry or a hotline report. For example, the provider’s counsel can contact an investigator or hotline caller (if not anonymous) to build a rapport and level of trust that will increase the flow of communication and help the provider gain a better understanding of the issue. Also, when a government agency is involved, counsel can telegraph the provider’s commitment to compliance by providing an appropriate level of assistance to the investigation. This may help dispel any of the agency’s concerns regarding the provider’s intent.

Keep in mind that the initial allegations may only be the tip of the proverbial iceberg, and the scope of the investigation may expand as it evolves. As explained below, it is important to take a broad view of the allegations and err on the side of being over-inclusive in document preservation efforts.

Collect and preserve information

The preservation of records and materials is serious business. A provider can face severe criminal consequences for the destruction of documents related to a compliance violation. Prior to Enron, many believed that preservation of records only became an issue once a federal investigation was initiated. Today, it is enough to be on notice of the possibility that an investigation may take place. Therefore, the provider should take immediate action to preserve and collect relevant documentation in appropriate circumstances. In nearly every such case, it will be necessary to work with IT professionals to preserve e-mail and hard drive information before it is inadvertently destroyed through routine purging exercises.

In addition, it is usually necessary to distribute a document preservation memo to all employees of the organization who have custody or control of relevant documents. Although a memo cannot stop an employee from improperly destroying documents, it can help show that the employee was acting unilaterally in defiance of company directives.

Conduct a thorough investigation

Once the relevant documents have been preserved, they must be gathered, reviewed, and evaluated at the direction of counsel. These tasks should be performed by individuals who were not involved in the events under investigation. Investigators often wait until the relevant documents are collected before conducting interviews, but in some circumstances, it makes more sense to conduct initial interviews to help identify the relevant documents.

Continued on page 7
The role of internal investigations: ...continued from page 5

While conducting interviews, care must be taken to preserve the integrity and privileged nature of the information obtained. The employment of counsel, especially counsel versed in internal investigations, greatly enhances the interview process. Counsel can compartmentalize information obtained in witness interviews to avoid cross-contamination of information and possible breaches of confidentiality. Also, counsel can advise employees (sometimes called “civil Miranda advisements”) that they are counsel only to the provider organization (or the authorizing committee) and do not represent the employee, that the employee’s truthful cooperation is expected, and that the employee is expected to maintain the confidentiality of the interview in order to protect the provider’s attorney-client privilege. In addition, counsel will explain that the attorney-client privilege belongs to the provider organization. Accordingly, the provider has the right to unilaterally waive the privilege, and it could choose to share the information obtained in the interview with others, including government agencies and regulators.

If an investigation concludes with a finding of non-compliance, the provider should undertake remediation efforts tailored to the conduct at issue.

Take remedial action
Remediation, broadly defined, is a key factor in mitigating penalties. Although the specifics of a remediation plan will vary from case-to-case, virtually all remediation plans include:
- ending non-compliant conduct;
- improving deficient procedures, policies, controls, and systems; and
- conducting training.

In some cases, remediation may call for refunding monies to the Fiscal Intermediary or other entities. In the context of a matter under self-disclosure to OIG, however, such refunds generally should be made only after approval by OIG.³

Training is essential to prevent future occurrences of the same conduct. In addition, it demonstrates the provider’s commitment to compliance. Training may be conducted by in-house experts or by a variety of consultants. Alternatively, organizations may seek training from web-based sources, because online interactive systems provide maximum training flexibility for the employee while ensuring that management is meeting its obligations for the organization’s compliance and recordkeeping. One such system, the Holland & Hart Compliance Management System (HHCMS), provides the additional benefit of generating test results and other forms of “defensive data” each time a user accesses the system. This data is stored for later retrieval to support audits and reviews. This defensive data strategy maximizes the use of compliance resources, because it not only documents the achievement of the training objective, but also generates data to address issues in the event of an audit or dispute.

At times, the situation may call for a provider to take disciplinary action against its employees, up to and including termination. The provider should take care to follow its established procedures for such action. In addition, care should be exercised to ensure that no discriminatory action is taken against employees who have reported compliance issues, as long as the reports were made in good faith.

Audit to verify remedial effectiveness
Simply implementing remedial action is not enough. The provider should demonstrate that remedial action has been effective by keeping a convincing audit trail. Without one, it is less likely OIG (or other regulators) will accept the voluntary measures undertaken as a substitute for more active governmental intervention and monitoring. It may be necessary to engage appropriate independent consultants to conduct the auditing activities to ensure objectivity and adherence to the required protocols.⁴

Penalties and CIAs
Regulators in the health care industry have an array of penalties available to address compliance violations, including the imposition of a Corporate Integrity Agreement (CIA). The government has the option to settle civil fraud and abuse claims, and because OIG has permissive exclusion authority under 42 U.S.C. § 1320a-7(b)(7), it may be in a provider’s interest to negotiate a settlement, including a CIA, with the government. In cases with mitigating factors, the provider may be able to negotiate a Certification of Compliance Agreement (CCA) or a lesser concession.³

CIAs usually impose stringent conditions on providers, including frequent auditing to track the effectiveness of the provider’s remedial efforts for a period of time lasting up to five years. More comprehensive CIAs may require the provider to:
- hire a compliance officer or appoint a compliance committee;
- develop written standards and policies;
- implement a comprehensive employee training program;
- review claims submitted to Federal health care programs;
- establish a confidential disclosure program;
- restrict employment of ineligible persons; and
- submit a variety of reports to the OIG.

CCAs, on the other hand, are less restrictive – generally requiring the provider to maintain its existing compliance program and provide a variety of reports on its compliance activities throughout the duration of the CCA. Where violations are less significant, a provider may

Continued on page 9
be able to avoid the imposition of CIAs or CCAs by showing that it has already implemented effective compliance measures on a voluntary basis.

Self-disclosure
The imposition of penalties and CIAs can be costly, time consuming and intrusive, but they may be avoidable. An effective compliance plan is a provider's first line of defense. It is therefore in a provider's best interest to have a compliance plan in place before an investigation is ever triggered. By having an early detection system in place, a provider can catch noncompliant activity and be in the position to voluntarily disclose it, when appropriate.

It is not always clear whether self-disclosure is appropriate. For example, it may not be clear whether a billing error is the type that should be disclosed to the OIG or whether it should be handled instead by the Fiscal Intermediary through its voluntary refund process. If a voluntary refund is made, but the Fiscal Intermediary turns around and reports the matter to OIG, that report may trigger a government investigation. On the other hand, providers are understandably loath to endure the disruption of an internal investigation and self-disclosure for a simple billing error that should properly be resolved through a voluntary refund. Timely advice from counsel may be helpful to resolve such issues without undue expense or exposure.

Voluntary self-disclosure has several benefits. OIG encourages the health care industry to conduct self-evaluations and self-disclosures. Accordingly, providers who make self-disclosures and demonstrate a good-faith effort to cooperate with OIG are in a position to minimize their potential civil, criminal, and administrative penalties. Additionally, providers that self-disclose are less likely to have to enter into a CIA or CCA. OIG believes that this presumption in favor of not requiring a compliance agreement appropriately recognizes the provider's commitment to integrity and also advances OIG's goal of expediting the resolution of self-disclosures. OIG is less inclined to impose CIA or CCA requirements on a provider who submits a complete and informative disclosure, responds quickly to OIG's requests for further information, and performs accurate audits. Such a provider has already adopted an effective compliance plan, so there is no compelling need for OIG to impose an additional one. Self-disclosure also creates an opportunity for the provider to conduct its own audit in conformance with OIG guidance. This can save time and money and provide a higher level of confidentiality and discretion.

The benefits of disclosure must be weighed against significant risks. OIG does not guarantee immunity or any other kind of benefit under its self disclosure protocol. Also, by making a self-disclosure, the provider may trigger a process that leads OIG to discover other violations not known to the provider. Furthermore, by disclosing the report of its internal investigation to OIG, the provider risks waiving any confidentiality or privilege protection otherwise applicable to the report and potentially even risks protection for underlying documents. Such a waiver could make the information available to third-parties for the purpose of collateral litigation. Finally, the OIG now requests a more complete initial submission that must be completed within three months after acceptance into the Self-Disclosure Protocol (SDP). To improve the disclosure process the initial submission must contain:

- a complete description of the conduct being disclosed;
- a description of the provider's internal investigation or commitment regarding when it will be completed;
- an estimate of the damages to the federal health care programs and the methodology used to calculate that figure or a commitment regarding when the provider will complete such estimate; and
- a statement of the laws potentially violated by the conduct.

As a result, providers are now under even more time pressure when considering self-disclosure as an option. For all these reasons, self-disclosure is a decision warranting careful consideration and counsel.

Conclusion
OIG seeks to enhance the integrity of the federal health care programs by encouraging meaningful compliance programs and self-disclosure of violations. However, compliance officers should not wait for a self-disclosure event to improve upon their existing programs. Instead, they should review their programs on an ongoing basis, both to enhance the program's design and to ensure its full implementation.

Even organizations with effective programs may experience incidents of noncompliance that require self-disclosure. Indeed, one of the hallmarks of an effective program is the ability to shine light on such incidents and use them as a means to identify underlying flaws and weaknesses for remediation.

Self-disclosure is becoming more common and attractive for the reasons outlined above. When a decision is made to disclose, compliance officers can position the matter for a more favorable outcome by demonstrating the organization's genuine commitment to compliance. The persuasiveness of that effort will be enhanced by the officer's ongoing attention to the organization's compliance program as discussed above.

---