Effective use of the OIG Voluntary Disclosure Protocol

By Daniel S. Reinberg, Esq.

Editor's note: Daniel S. Reinberg is a partner with Foley & Lardner LLP in Chicago. He has represented numerous health care providers concerning fraud and abuse issues. He is a former Assistant United States Attorney for the Northern District of Illinois. He can be reached by telephone at 312/832-5167 or by e-mail at dreinberg@foley.com.

It is inevitable that, at one time or another, health care providers will find that they have received an overpayment from a government payor. Often these overpayments are the result of innocent mistakes and not the result of fraud or program abuse. The provider has no legal entitlement to keep an overpayment but, surprisingly, hospital administrators often remark that the decision of whether to disclose and repay the overpayment is one of the most difficult decisions they face. Given the potential for criminal prosecution as a result of failing to disclose a known overpayment, the decision ought not to be so difficult.

This first section of this article discusses the potential sources and theories of criminal liability for failure to disclose known overpayments, even if those overpayments are received through an innocent mistake. The next section provides a summary of the benefits and risks for providers who make a voluntary disclosure, and the final section sets forth some practical guidance concerning how and when to make a voluntary disclosure and conduct an audit under the U.S. Department of Health and Human Services, Office of Inspector General's Self-Disclosure Protocol ("Protocol").

Sources of criminal liability for failure to disclose known overpayments

The decision whether to voluntarily disclose overpayments must start with an assessment of the potential consequences stemming from a failure to make such a disclosure. Beyond monetary and administrative penalties, federal law imposes substantial criminal penalties for failure to disclose even innocently obtained overpayments. Some of the most pertinent criminal statutes are discussed below.

Failure to Disclose Receipt of Excess Benefits. Perhaps the single most relevant statute concerning a provider's obligation to disclose known overpayments is Section 1128B(a)(3) of the Social Security Act (42 U.S.C. § 1320a-7b(a)(3)), which provides in pertinent part:

> [W]hoever having knowledge of the occurrence of any event affecting (A) his initial or continued right to any such benefit or payment . . . conceals or fails to disclose such benefit or payment either in a greater amount or quantity than is due or when no such benefit or payment is authorized, . . . [shall be punished].

This statute has been interpreted (albeit not unanimously) as imposing an affirmative obligation to disclose Medicare and Medicaid overpayments and provides for criminal liability for the failure to do so. While the statute requires disclosure, it does not require repayment. Violation of this statute is a felony punishable by a maximum of five years in prison and a fine of $250,000 for individuals or $500,000 for corporations.

OIG interprets this statute as requiring disclosure of known overpayments. [See e.g., OIG Compliance Guidance for Hospitals, 63 Fed. Reg. 8,987, 8,998 (February 23, 1998)]:

> "…failure to repay overpayments within a reasonable period of time could be interpreted as an intentional attempt to conceal the overpayment from the Government, thereby establishing an independent basis for a criminal violation with respect to the hospital, as well as any individuals who may have been involved."

The government's view is that when a provider concludes it has received funds to which it is not entitled, subsequent retention of the funds is a "failure to disclose" with fraudulent intent. This argument is more or less consistent with the general approach of 42 U.S.C. § 1395g(a), which requires for the calculation of Medicare Part A benefits adjustments on account of previously made overpayments, but is still untested in the courts. OIG also is likely to view this statute as creating a "continued offense," meaning that each day in which a provider fails to disclose a known overpayment presents a new offense. Under this theory, the government could argue that overpayments received many years in the past, nonetheless, could result in current violations of Section 1320a-7b(a)(3) if known and not disclosed.

Section 1320a-7b(a)(3) is arguably ambiguous as to the meaning of the term

"fraudulently to secure." Thus, it is unclear whether a provider who innocently receives an overpayment develops the required fraudulent intent by failing to disclose the overpayment once the provider discovers it. OIG likely will advocate a violation of the statute under these circumstances, and no court has held to the contrary. While there is a single arbitration decision in connection with a private dispute between the Healthcare Financial Advisors, Inc. and Certus Corporation, in which a retired state court judge held that Section 1320a-7b(a)(3) does not apply to innocently obtained and non-recurring overpayments, the nonbinding effect of this arbitration decision and the potential criminal penalties involved make it too risky not to disclose known overpayments.

Criminal False Claim Act (FCA). Section 287 of Title 18 provides for imprisonment of up to five years, a fine, or both, for any person who "makes or presents" any claim to an agency of the U.S. Government "knowing such claim to be false, fictitious, or fraudulent." This statute applies where the victim is the U.S. Government, including the Medicare, Medicaid, and Tricare programs. There is no requirement that the submitted claim itself be false on its face, as the statute also includes "fraudulent" claims. In addition, conspiracies to violate Section 287 are criminalized by Section 286 of Title 18, and the penalties for conspiracy are twice as severe as what can be imposed under Section 287.

In general, the same type of conduct that produces violations of the civil False Claims Act (31 U.S.C. § 3729 et seq.) could lead to criminal liability under Section 287 for providers who fail to disclose known overpayments. Under the FCA, a person may be liable for knowingly submitting a false or fraudulent claim for payment to the government. In order to impose liability, the government must prove that a "false or fraudulent" claim was "knowingly" submitted for payment or that a "false record or statement" was made in order to get a false claim paid or approved [31 U.S.C. §§ 3729(a)(1) and (2)]. Notably, even in instances where an overpayment is obtained innocently, meaning that the initial claim submitted was not false on its face, FCA liability can attach under Section 3729(a)(1) based on conduct occurring after discovery of the overpayment. For instance, some courts have held that the endorsement and deposit of a government check—known to have been issued in error—constitutes presentation of a false claim and may subject the recipient to liability under the FCA. [See e.g., *United States v. McLeod*, 721 F.2d 282 (9th Cir. 1983).]

In addition, Section 3729(a)(7), which has become known as the "reverse false claim" provision, serves as a basis for liability if a person "knowingly makes, uses, or causes to be made or used, a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money" to the government. Under this section, a fraudulent attempt to reduce an amount owed to the government could constitute a false claim. Thus, if a provider retains money that it knows it owes to the government, the provider could be liable under Section 3729(a)(7). This argument seems particularly strong for Part A benefits in light of the language of 42 U.S.C.1395g(a), which indicates that ongoing Medicare payments are to include "necessary adjustments on account of previously made overpayments or underpayments . . ."

Health Care Fraud. Title 18, Section 1347 makes it a crime to knowingly and willfully execute (or attempt to execute) a scheme to defraud any health care benefit program, or to obtain money or property from a health care benefit program through false or fraudulent pretenses, representations, or promises. This statute applies to federal health care programs and most other health care benefit programs. The penalty for a violation of this statute may include fines, imprisonment of up to ten years, or both. The prison term may be increased where the violation results in serious bodily injury or death.

This statute has been recently used to prosecute individuals engaged in alleged schemes aimed at non-profit health maintenance organizations and private insurance companies. [See e.g., *United States v. Baldwin*, D.D.C. No. 02-0323 (PLF) (August 14, 2003) an indictment for a scheme to defraud Kaiser Foundation Health Plan Inc., a non-profit health maintenance organization; and *United States v. Murphy*, N.D. Tex, No. 4:02-CR-011-Y, in which a defendant physician was convicted in May 2003 of submitting more than one million dollars in fraudulent medical claims to insurance companies between 1996 and 2000 for services he did not provide or supervise at medical clinics located in health clubs.]

In the case of a failure to disclose a known overpayment, the government may view the failure to disclose the overpayment as evidence of fraudulent intent, present at the time the initial claims were submitted. In cases where the overpayment undeniably resulted from an innocent mistake, the government may still seek to define a "scheme" to defraud in terms of the concealment that occurs after knowledge of the overpayment. For instance, providers who are examined by outside auditors are routinely asked questions that should reasonably call for disclosure of an overpayment to the auditors. In instances where this information is withheld or false information is provided to the auditors, the government likely will view this as active concealment and, thus, evidence of a scheme to defraud beginning at least at the time of the concealment.

Other Federal Criminal Statutes. A host of other federal criminal statutes could be used

Continued on page 41

by the government to prosecute a health care provider (and/or individuals) for failure to disclose known overpayments. While not an exhaustive list, some of the most commonly used criminal statutes are:

- Mail Fraud (18 U.S.C. § 1341)
- Wire Fraud (18 U.S.C. § 1343)
- False Statements Relating to Health Care Matters (18 U.S.C. § 1035)
- Embezzlement of Public Money or Property (18 U.S.C. § 641)
- Embezzlement in Connection with Health Care (18 U.S.C. § 669)
- Concealment of Material Fact (18 U.S.C. § 1001)
- Misprision of a Felony (18 U.S.C. § 4)

Benefits and risks of making a voluntary disclosure

Disclosure of known overpayments is arguably mandatory, but the benefits of making a voluntary disclosure go well beyond simply complying with the law. By making a voluntary disclosure, providers often can obtain some or all of the following benefits:

- Disclosure may help a provider avoid a referral for criminal prosecution.
- With a disclosure, the provider can place the misconduct in the best light, assert defenses, and argue mitigating circumstances.
- Disclosure may persuade the government to forego a formal investigation, particularly where the provider has taken appropriate remedial action.
- Disclosure may result in reduced civil and administrative fines and penalties, including the avoidance of a corporate integrity agreement.
- Effective disclosure can reduce the possibility that the government investigation will be broad, unfocused, and needlessly burdensome.
- With a government release, a *qui tam* relator will be barred from bringing a whistleblower action.

Voluntary disclosures, however, are not without risk. Some disadvantages to disclosure are that:

- No guarantee of leniency from the government is exchanged for the voluntary disclosure.
- Disclosure may alert the government to possible wrongdoing that is otherwise unknown and lead to criminal prosecution.
- Disclosure may provide a roadmap for the government's investigation.
- Disclosure sets in motion a chain of events over which the provider has little control, such as more extensive audits and reviews of the provider's practices.
- Disclosure may generate adverse publicity.
- The provider may have to waive the attorney-client privilege and attorney work-product doctrine protection with respect to the entire investigation (or portions thereof).
- For publicly traded providers, the potential for shareholder suits and derivative actions increases.
- Employee morale may be affected negatively and employees may be less likely to cooperate in future investigations.
- Disclosure will cost the company time, money, and employee productivity.

Experience has demonstrated that a truly voluntary, timely disclosure will be viewed more favorably by the government than a violation that is uncovered through a government routine or targeted audit or as a result of a whistleblower's tip. Indeed, to date there have been 321 voluntary disclosures accepted by OIG under the Protocol. Of these disclosures, 137 were resolved with a monetary payment and only 23 resulted in a corporate integrity agreement. [See Report on Medicare Compliance, Volume 16, No. 17 at 1 (May 7, 2007).]

When and how to make a disclosure

Disclosures under the OIG Protocol are reserved for overpayments in which potential civil or criminal penalties may be attached. Ordinary overpayment should be resolved through the relevant Medicare contractor. As such, providers clearly should use the Protocol under circumstances that could amount to fraud or intentional misconduct. Likewise, where the dollar amount of a series of overpayments is significant or occurred over a lengthy period of time, the provider risks being judged as reckless, thereby triggering potential civil liability under the False Claims Act. Under these circumstances, the Protocol may be invoked.

A variety of issues have been disclosed under the Protocol, including but not limited to: (1) billing for medically unnecessary services; (2) billing for services performed by an excluded individual; (3) evaluation and management (E&M) upcoding; (4) diagnosis-related group (DRG) upcoding; (5) duplicate billing; (6) alteration or falsification of records; and (7) kickbacks and/or Stark violations. Disclosure of Stark violations under the protocol can be very advantageous in that, as set forth in a recent open letter to health care providers, OIG will resolve these disclosures based on a multiple of the value of the financial benefit conferred by the provider, as opposed to a multiple of the amount of the claims submitted for services provided by the tainted physician. Given OIG's jurisdictional limitations, such disclosures of Stark violations must include an admission of intentional misconduct.

Once a decision has been made to make a voluntary disclosure to OIG, the process for doing so under the Protocol is rigid and must be followed. The disclosure must be in writing and mailed to the Assistant Inspector General for Investigative Operations, Office of Investigations. The disclosure must include certain facts, including basic information about the provider, whether a government investigation already exists, and a full description of the

Continued on page 43

matter disclosed (which typically includes the types of claims involved, the individuals or entities involved, their respective roles, and the relevant time periods). A provider need not wait until its internal investigation is complete before making a voluntary disclosure under the Protocol. However, the provider must have conducted enough of the investigation to set forth these basic facts in its initial letter. The OIG recommends that, in order to demonstrate their "good faith and willingness to work with the government to correct and remedy the problem," providers must report the matter to the OIG within 60 days after receipt of "credible evidence of misconduct." [See OIG Model Compliance Plan for Clinical Laboratories, February 14, 1997, § G(l)(b).]

At the conclusion of the internal investigation, the Protocol requires the disclosure of an internal investigation report and lists the required elements of that report. The report must contain a quantification of the potential liability to the government (including detailed statistical sampling requirements), the names of all persons interviewed, summaries of the interviews, and the identification of personnel within the disclosing entity that "should have known of, but failed to detect, the incident or practice based on their job responsibilities." The written submission should also include a certification by an authorized representative of the disclosing entity that the contents of the disclosure are truthful.

After disclosure pursuant to the Protocol, OIG will begin verification of the information provided. OIG states that it must have access to all audit work papers and other supporting documents without the assertion of privileges. However, OIG states that it will not "normally" ask for production of written communications subject to the attorney-client privilege. It is important to note that OIG is not bound by the provider's findings and will independently assess the evidence. This assessment can include interviews of key witnesses, review of documents, and assessment of audit procedures and results.

Audits to quantify the financial impact of billing errors are a critical step in the process. The Protocol has very specific guidelines as to how these audits must be conducted. The Protocol requires the use of a specific statistical sampling method involving a probe sample followed by, if appropriate, a full sample. The Protocol recommends the use of RAT-STAT (a package of statistical software tools used by the U.S. Office of Audit Services in the Department of Health & Human Services) for purposes of sample selection. When supervised by experienced legal counsel, external consultants are often utilized to conduct these audits for purposes of independence and statistical expertise.

In reporting results of an investigation to OIG under the Protocol, it is equally important to report facts that show that corrective actions have been taken and that the provider's compliance program is operating effectively. The development of these facts is critical to avoid the imposition of a corporate integrity agreement or other independent monitoring obligations.

Conclusion

Significant risks and benefits must be factored into the decision to disclose a known overpayment. While the facts of each case will be determinative, given the legal framework described above, in most cases when an overpayment is discovered, the better course of conduct is to take immediate corrective action, including disclosing the past misconduct and making reparation for an appropriate period and in an appropriate amount. How and when the disclosure is made will vary from case to case, depending upon the circumstances, though in recent years, providers have obtained positive results through the OIG Self-Disclosure Protocol. ■

where the people truly participate, you don't need control. They know what needs to be done, and they do it. And the more that people will devote themselves to your cause on a voluntary basis, a willing basis, the fewer hierarchies and control mechanisms you need. We're not looking for blind obedience. We're looking for people who, on their own initiative, want to be doing what they're doing because they consider it to be a worthy objective. I have always believed that the best leader is the best server. And if you're a servant, by definition, you're not controlling."

The rationale for centralized, top-down decision making (i.e., control, direction, and compliance) melts away when individuals are tightly aligned with the company's values and goals, accountable for their actions, and self-regulated. Because values-based governance is positive governance—given to what is desirable rather than what is prohibited—it presents a proactive solution to achieving corporate aims. As opposed to the heavy enforcement apparatus of blind obedience cultures or the reactive, make-another-rule solution of informed acquiescence, values-based self-governance provides constitutional principles that can be applied again and again to situations as they arise. It addresses the wide range of possible human conduct more comprehensively and puts the values of the company out in front of behavior. ■

This article includes a section of the book "HOW: Why How *We Do Anything Means Everything…in Business (and in Life)" written by Dov Seidman. It is excerpted with permission of the publisher John Wiley & Sons, Inc. © 2007 by Dov Seidman. This book is available at bookstores, online booksellers, and from the Wiley Web site at www.wiley.com, or 800/225-5945.*