Fox Rothschild LLP
ATTORNEYS AT LAW

Staying Well Within the Law

A newsletter on the current legal issues facing today's health care industry

Fourth Quarter 2011

You Spoke, They Listened: The Interim Final ACO Rule

By William H. Maruca

The proposed Medicare Shared Savings rule for Accountable Care Organizations (ACOs) landed with a thud when it first appeared in March 2011. The rules implementing this highly anticipated program were considered overly burdensome and the potential economic upside too uncertain. The prototype health systems that served as the models for the initiative, including Marshfield Clinic and Geisinger Health System, declined to participate without major changes. More than 1,300 comments were filed with the Centers for Medicare and Medicaid Services (CMS). Were ACOs DOA?

To paraphrase Mark Twain, the reports of ACOs' demise were at least somewhat exaggerated. In an unusual display of responsiveness, CMS and its sister regulatory agencies adopted nearly all of the recommendations requested by major health care provider advocates and may have breathed new life into a program that had been given up by many as another casualty of government overreaching.

The 2009 Patient Protection and Affordable Care Act (ACA) authorized the Shared Savings program under which qualifying ACOs would be eligible for additional Medicare payments if they achieved savings over historical costs while maintaining quality criteria. An ACO would coordinate all care needed by a pool of at least 5,000 designated Medicare fee-for-service patients. ACOs must include primary care providers and generally would also include specialists, hospitals and ancillary care providers. The proposed rule drew sharp criticism for its requirement that all ACOs share downside risk; the retrospective method of identifying patients whose costs would be tracked, and the lengthy list of quality measurements and statistics that were required to participate in the program, among other concerns.

On October 20, 2011, an advance copy of the interim final ACO rule was released. It was published in the *Federal Register* on November 2, 2011. Among the changes agreed to by CMS were the following:

• Downside Risk

In the proposed rule, ACOs could choose from two three-year tracks with two levels of shared savings, but both tracks required the ACO be liable for downside risk no later than year three. This proved highly unpopular, particularly with the 10 practices that had participated in the Physician Group Practice demonstration program, which had no downside risk. The final rule has eliminated the risk exposure from Track 1, and ACOs under this option will not be exposed to liability for failure to achieve cost savings. Track 2 would entitle ACOs to a higher percentage of shared savings in exchange for assuming downside risk from year one and would likely only appeal to large, fully integrated ACO applicants.

• Patient Assignment

ACOs need to manage costs with regard to identified patient pools. The proposed rule would have attributed patients to an ACO at the end of each performance year based on whether those patients had utilized that ACO's members for most of their primary care services during that year. This was intended to assure fairness so that an ACO was not penalized for costs incurred out of its network, keeping in mind that patients have no restrictions on where to obtain care. Commenters suggested that a retrospective system would force them to manage costs in the dark, without knowing what costs they would be ultimately responsible for. In the final rule, CMS opted for a modified system under which ACOs are given a preliminary list of prospective Medicare beneficiaries at the beginning of a performance year based on those beneficiaries' past use of primary care services, and that list would be reconciled quarterly based on the actual primary care use during the year. It is hoped this approach would allow ACOs to carefully monitor the costs they are incurring for their assigned patients without being held accountable for costs incurred elsewhere if the patient leaves the network mid-year. It is not a foolproof solution, in that a patient could get his or her primary care from an

In This Issue:

ACO member but seek more expensive specialist and hospital care from non-ACO members.

• Quality Measures

ACOs would have been required to track and report on 65 separate quality measures under the proposed rule and demonstrate improvement or meet performance goals beginning in the second year. The cost and infrastructure required to track these criteria was intimidating to many commenters. In response, CMS reduced the number of quality measures from 65 to 33 and agreed to a longer phase-in for the pay-for-performance elements of the rule.

• Savings Formula

ACOs participating in proposed Track 1 would only share savings in excess of two percent over defined benchmarks. CMS sweetened the pot by eliminating the two percent threshold for both tracks in the final rule. Now, all ACOs will share in first dollar savings once a minimum savings rate has been achieved. Importantly, the proposed "performance payment withhold" of 25 percent of shared savings has been removed. This provision was widely criticized as disproportionately penalizing the most successful ACOs without providing any meaningful security for the struggling ACOs. (It is also now unnecessary for Track 1, which no longer includes any downside liability exposure). CMS will now rely on a provision under which each ACO applicant participating in Track 2 will be required to demonstrate that it has established a repayment mechanism and specify how the liability for sharing losses would be spread among ACO participants and/or ACO providers/suppliers. CMS will determine the adequacy of an ACO's repayment mechanism prior to the start of each performance year under the two-sided model.

• Start Date

Recognizing there would be no way for the program to be operational by January 1, 2012, CMS modified the start dates so ACOs can join on April 1, 2012, or July 1, 2012, with the first performance period extended to 18 or 21 months, then reverting to the calendar year. Applications will be accepted in early 2012.

• Electronic Health Records

One controversial provision of the proposed rule would have required an ACO to verify that 50 percent of its members met the HITECH Act's "meaningful use" standards for electronic health records (EHR). The final rule drops the 50 percent requirement but ranks meaningful use as its highest-weighted quality measure to continue to ensure the adoption of EHR. In reality, it would be unlikely that an ACO could achieve savings or quality goals without robust use of EHR systems.

• Advance Payment

ACOs aren't cheap to develop. CMS' Innovation Center developed an Advance Payment ACO Model to allow certain ACO participants in the Shared Savings Program to receive advance payments that will be recouped from the shared savings they earn. Under the Advance Payment ACO Model, participating ACOs will receive an upfront, fixed payment; a variable payment based on the number of its historically-assigned beneficiaries; and a monthly payment of varying amount depending on the size of the ACO and the number of its historically assigned beneficiaries The model is designed to provide support to ACOs whose ability to achieve the three-part aim would be improved with additional access to capital, including rural and physician-owned organizations. Only ACOs that do not include any inpatient facilities **and** have less than $50 million in total annual revenue, and ACOs in which the only inpatient facilities are critical access hospitals and/or Medicare low-volume rural hospitals **and** have less than $80 million in total annual revenue will qualify, but not those that are co-owned with a health plan.

• Antitrust Guidelines

Along with CMS' rule, the federal antitrust enforcement agencies (Department of Justice and Federal Trade Commission) eliminated their prior requirement for mandatory review but will offer voluntary expedited review within 90 days. They clarified the safety zones and the method for determining market share based on each participants' Primary Service Area (PSA) and also clarified the rural exception and rules for "dominant participants" with greater than a 50 percent share of a service within a PSA. Critics (particularly insurance companies) have already suggested these changes will lead to greater concentration and market power among large entities that will then be able to raise prices.

• Stark and Anti-Kickback

The Stark/Anti-Kickback/Civil Monetary Penalties waivers were expanded to protect ACO activities in five different categories: ACO pre-participation; ACO participation; shared savings distribution; compliance with self-referral/waiver of gainsharing; and patient incentives.

• Tax Considerations

Finally, the IRS revised its policy on the impact of participation in the Shared Savings Program on tax-exempt entities. The IRS will apply a case-by-case analysis based on facts and circumstances but sets forth a list of criteria that, if met, will result in no private inurement/private benefit. The IRS remains concerned about tax-exempt participants in ACOs bearing a disproportionate amount of costs compared to their relative investments.

What Next?

The industry got its wish list fulfilled. In early 2012 we will begin to see if these concessions have incentivized a sufficient level of participation in the ACO Shared Savings Program to vindicate those, like outgoing HHS Administrator Dr. Donald Berwick, who have staked the future financial solvency of Medicare on efforts to end pay-for-volume and transition to pay-for-results.

For more information about this topic, please contact William H. Maruca at 412.394.5575 or wmaruca@foxrothschild.com.

SAIC and Its Military Millions March: Flooding the Parade with Possible PHI Breaches

By Elizabeth G. Litten and Michael J. Kline

The largest single protected health information (PHI) breach reported to date – involving almost 5,000,000 military clinic and hospital patients – highlights the complexities in the decision-making process that covered entities and business associates should employ with respect to notifying the Department of Health and Human Services (HHS), other regulators and potentially affected individuals of a PHI breach. It may also ultimately provide covered entities and their business associates with valuable information and guidance when confronting a large PHI breach as well as test the regulatory boundaries preventing private actions under HIPAA/HITECH.

The 2011 breach, publicly disclosed in a statement on September 29, 2011 (the Public Statement), involved Science Applications International Corporation (SAI-NYSE) (SAIC) and occurred in the context of the company's role as a business associate and/or subcontractor for TRICARE Management Activity, a component of TRICARE, the military health plan (TRICARE), for active duty service members of the U.S. Department of Defense (DoD). According to a recent filing by SAIC posted on the SEC web site, SAIC describes itself as "a FORTUNE 500® scientific, engineering and technology applications company that uses its deep domain knowledge to solve problems of vital importance to the nation and the world, in national security, energy and the environment, critical infrastructure and health." SAIC has an estimated 41,000 employees who serve customers in the DoD, the intelligence community, the U.S. Department of Homeland Security, other U.S. government civil agencies and selected commercial markets.

The PHI that was compromised was reported as having been contained on backup tapes used by the military health system. SAIC noted in its Public Statement that the PHI "may include Social Security numbers, addresses and phone numbers, and some personal health data such as clinical notes, laboratory tests and prescriptions" but no financial data, such as credit card or bank account information, was contained on the tapes. SAIC reported the breach despite the fact that the PHI was contained on backup tapes and, as explained in the Public Statement, in SAIC's view, "The risk of harm to patients is judged to be low despite the data elements involved since retrieving the data on the tapes would require knowledge of and access to specific hardware and software and knowledge of the system and data structure…"

To Report or Not To Report?

SAIC apparently debated over whether to notify the nearly 5,000,000 affected individuals about the breach. It is important to note that the HITECH Breach Notification Interim Final Rule defines a "breach" as "the acquisition, access, use or disclosure of … PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information." It further explains that "compromises the security or privacy of the protected health information" means "poses a significant risk of financial, reputational or other harm to the individual." Additionally, it defines the term "access" for purposes of the interim final rule as "the ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource."

These definitions raise an important issue: At what point does "access" matter? When is the mere "ability" to read PHI, without evidence the PHI was actually read or was likely to have been read, enough to trigger the notice requirement under the Breach Notification Rule? Will covered entities provide notice out of an abundance of caution to report every unlocked or unencrypted data file, possibly flooding the HHS web site that lists large PHI breaches with potential breaches that have minimal or no likelihood of access and unduly alarming notified individuals? Could such reporting have the unintended effect of diluting the impact of reports involving actual theft and snooping?

In this regard, an event reported on the Nemours Web site on October 7, 2011 (the Nemours Report), about a PHI security breach involving approximately 1.9 million individuals at a Nemours health care facility in Wilmington, DE, is relevant. The Nemours Report stated that three unencrypted computer backup tapes containing patient billing and employee payroll were missing. The tapes reportedly were stored in a locked cabinet following a computer systems conversion completed in 2004. The tapes and locked cabinet were reported missing on September 8, 2011, and were believed to have been removed on or about August 10, 2011, during a facility remodeling project. The Nemours Report stated, "There is no indication that the tapes were stolen or that any of the information on them has been accessed or misused. Independent security experts retained by Nemours determined that highly specialized equipment and specific technical knowledge would be necessary to access the information stored on these backup tapes. There are no medical records on the tapes."

The Nemours Report reveals that, in spite of the low likelihood of access, it not only disclosed the breach but was offering free credit monitoring, identity theft protection and call center support to affected individuals.

If the analysis as to whether access "poses a significant risk of … harm" takes into account the likelihood that PHI was

actually accessed, rather than simply whether a theoretical "ability or means" to read, write, modify or communicate PHI existed at some point in time, perhaps the "possible breach" floodgates will not burst open unnecessarily.

SAIC ultimately decided to notify all potentially affected individuals of the breach. The Public Statement noted, "After careful deliberation, we have decided that we will notify all affected beneficiaries. We did not come to this decision lightly. We used a standard matrix to determine the level of risk that is associated with the loss of these tapes. Reading the tapes takes special machinery. Moreover, it takes a highly skilled individual to interpret the data on the tapes. Since we do not believe the tapes were taken with malicious intent, we believe the risk to beneficiaries is low. Nevertheless, the tapes are missing and given the totality of the circumstances, **we determined that individual notification was required in accordance with DoD guidance**. . . " [Emphasis added.]

The linchpin of SAIC's final decision to notify appeared to be the DoD guidance. In SAIC's position as an $11 billion contractor heavily dependent on DoD and other U.S. government agencies, the company may not have had many practical alternatives but to notify beneficiaries. SAIC's "careful deliberation" resulted in the conclusion that the risk of breach was "low." Had the DoD guidance not been a factor and had SAIC concluded the case was one where an unlocked file or unencrypted data was discovered to exist — but it appeared that no one had opened such file or viewed such data — would SAIC's conclusion have been the same and would it, like Nemours, have decided to report it?

Rapid About-Face on Credit Monitoring

SAIC and TRICARE, according to the Public Statement, are cooperating in the notification process but initially told all potentially affected individuals that no credit monitoring or restoration services would be provided in light of the "low risk of harm." This was in contrast to the decision of Nemours in the Nemours Report to provide such services. The Public Statement noted that, "To date, we have no conclusive evidence that indicates beneficiaries are at risk of identity theft, but all are encouraged to monitor their credit and place a free fraud alert of their credit for a period of 90 days using the Federal Trade Commission (FTC) web site."

However, less than six weeks later, TRICARE directed SAIC to provide one year of credit monitoring and restoration services to patients "who express concern about their credit" as a result of the PHI breach. A press release issued by the DoD on November 4, 2011, noted, "These additional proactive security measures exceed the industry standard to protect against the risk of identity theft. We take very seriously our responsibility to offer patients peace of mind that their credit and quality of life will be unaffected by this breach."

It is unclear whether the new security measure actually exceeds the "industry standard," as, in numerous reported PHI breaches, including Nemours, up to two years of credit monitoring was offered to affected individuals. However, given the original assurances in the Public Statement that the risk of harm was low and there was no conclusive evidence that patients were at risk of identity theft, one can speculate as to whether TRICARE's abrupt about-face relates to new evidence, a revised judgment as to the risk of harm to affected patients and/or simply an abundance of caution as to its own exposure to risk.

Then again, TRICARE's new position could have less to do with new concerns related to patient identity theft risk and more to do with a "proactive response" or even a preemptive strike by TRICARE and the DoD to combat some of the allegations in the putative class action lawsuit filed against them in the U.S. District Court for the District of Columbia on October 11, 2011 (*Gaffney v. TRICARE Management Activity, et. al.*, Case No. 1:2011cv01800), where plaintiffs allege they have "incurred an economic loss as a result of having to purchase a credit monitoring service to alert [them] to potential misappropriation of their identity."

By offering the credit monitoring services to all of the 4.9 million affected individuals, TRICARE and the DoD may be endeavoring to render moot or at least mitigate the risk from those allegations in the class action complaint, which seeks judgment against TRICARE and the DoD for damages in an amount of $1,000 for each affected individual. Some quick math indicates that the cost of credit monitoring and restoration for a subset (those "expressing concern") of the roughly 4.9 million affected patients would be far less than the almost $5 billion aggregate damages award sought in the putative class action complaint. TRICARE may have reversed its stance as a result of this "risk of harm" analysis and not because of new information or a revised evaluation related to a heightened risk of harm to affected individuals.

There is also another putative class action that has been filed separately against SAIC (but not TRICARE and the DoD) in respect to the breach.

History of Breaches?

A closer review of SAIC and its incidents involving PHI reveals that the 2011 breach was not the first for the company. It does, however, appear to be the first since the adoption of the HITECH Breach Notification Interim Final Rule in August 2009.

On July 21, 2007, *The Washington Post* reported that SAIC had acknowledged the previous day that "some of its employees sent unencrypted data — such as medical appointments, treatments and diagnoses — across the Internet" that related to 867,000 U.S. service members and their families. The *Post* article stated that, "So far, there is no evidence that personal data has been compromised, but 'the possibility cannot be ruled out,' SAIC said in a press release. The firm has fixed the security breach, the release said." Embedded later in the *Post* article is this: "The [2007] disclosure comes less than two years after a break-in at SAIC's headquarters that put Social Security numbers and other personal

information about tens of thousands of employees at risk. Among those affected were former SAIC executive David A. Kay, who was the chief U.N. weapons inspector in Iraq, and a former director who was a top CIA official." It is unclear whether the earlier 2005 breach reported in the *Post* involved PHI or other personal information.

On January 20, 2009, SPAMfighter reported SAIC had informed the Attorney General of New Hampshire of a data breach that had occurred involving malware. The SPAMfighter report notes SAIC wrote a letter to many affected users to inform them about the potential compromise of personal information. (A portion of such personal information would have been deemed PHI had it been part of health-related material.) The SPAMfighter report also discloses that, "The current [2009] breach at SAIC is not the only one. There was one other last year (2008), when keylogging software managed to bypass SAIC's malware detection system. That breach had exposed mainly business account information."

Final Thoughts

The SEC issued a release on October 13, 2011, containing guidelines for public companies regarding disclosure obligations relating to cybersecurity risks and cyber incidents. In the context of SAIC, an $11 billion company, while the actual costs of notification and remediation of the 2011 Breach may run into millions of dollars, the 2011 Breach may not be deemed a "material" reportable event for SEC purposes by its management.

It is likely that much more will be heard in the future about the mammoth 2011 SAIC breach and its aftermath that may give covered entities and their business associates valuable information and guidance to consider in identifying and confronting a future large PHI security breach. The regulatory barriers preventing private actions under HIPAA/HITECH may be tested by the putative class action lawsuits. It will also be interesting to see whether the cooperation of SAIC with TRICARE and the DoD may wither in the face of the pressures of the lawsuits.

For more information about this topic, please contact Elizabeth G. Litten at 609.895.3320 or elitten@foxrothschild.com or Michael J. Kline at 609.895.6635 or mkline@foxrothschild.com.

This article previously appeared as a series of postings on the firm's HIPAA, HITECH and Health Information Technology blog (http://hipaahealthlaw.foxrothschild.com).

Will the SEC's Whistleblower Bounty Change Employer/Employee Relationships?

By David Restaino

Under regulations that took effect on August 12, 2011, the Securities and Exchange Commission (SEC) has given itself a new weapon to combat corporate fraud. In essence, whistleblowing employees in many different corporate environments have an incentive to notify the SEC of compliance issues—even if those employees have not utilized internal reporting systems—and earn themselves a huge reward.

The scope of the regulations is breathtaking. For example, if a publicly traded pharmaceutical company is illegally practicing off-label promotion of its products, a whistleblower who advises the SEC of this activity can receive up to 30 percent of a subsequent settlement of the allegations. Similarly, a private entity providing illegal kickbacks might, if it seeks to raise capital under certain Securities Act provisions, find itself subject to rules that protect a whistleblower from retaliation. With settlements in many fields—be it pharmaceuticals, health care or even violations of good manufacturing practices in the food and drug industry—exceeding hundreds of millions of dollars, and often billions, the impact of the new SEC rules will be immediate.

And that, apparently, is the whole point of Wall Street reform. While companies are already conversant in statutes like the False Claims Act and the Anti-Kickback Statute, which use back-end penalties as a disincentive to fraud, the SEC can now attack the issue of corporate fraud from the other end and use the people most likely to know about it (e.g., corporate employees) to root out the problem.

A Summary of the Whistleblower Rewards Rule

Pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act (Wall Street Reform Act), adopted July 21, 2010, the SEC was empowered to adopt rules providing incentives for whistleblowers and also to provide them protection from retaliation.[1] The SEC rules were published on June 13, 2011, and became effective on August 12, 2011.[2]

Under the SEC rules, a whistleblower may be eligible to receive a bounty or reward if he or she voluntarily provides original information that causes the SEC to commence an examination or open a successful investigation or if the information significantly contributes to an ongoing investigation. The information cannot have been demanded by the SEC or known by the SEC from another source when reported. There are additional eligibility requirements. Among other things, the disclosures must lead to the recovery of more than $1 million (including "related actions" such as those brought by state attorneys general or by certain federal agencies).

The bounty is certain to raise a few eyebrows. For starters, eligible

[1] Public Law No. 111-203 § 922(a) (to be codified at 15 U.S.C. § 78u-6 et seq.) and § 924.
[2] 76 Fed. Reg. 34,300 (June 13, 2011) (to be codified at 17 C.F.R. Part 240).

whistleblowers can get 10 to 30 percent of judgments that exceed $1 million, which should leave no doubt the Wall Street Reform Act will encourage litigation against corporations. The actual value of a reward will depend on a variety of factors enumerated in the SEC rules (i.e., the reliability, completeness and significance of the information provided, the degree to which it helped the enforcement action and other assistance given by the whistleblower). Moreover, there is no requirement that a complaining employee first resort to available corporate compliance programs. Stated differently, internal reporting is not a pre-condition to award eligibility.

But the SEC has provided some incentives for individuals to take advantage of internal corporate compliance programs: Voluntary participation in such programs increases the reward, and "full bounty credit" is given to persons whose internal efforts trigger a corporate disclosure to the SEC that results in a successful enforcement action.

The SEC rules are commonly viewed as applicable to public companies, but they go further. Also falling under the umbrella of the rules are broker-dealers and investment advisers as well as certain private companies seeking to raise capital under specified Securities Act provisions.

Fortunately, the SEC rules also contain some common sense exclusions, specifically that attorneys, directors, officers, compliance staff and internal audit personnel are generally ineligible for rewards. There are, of course, exceptions to the exclusions, and those exceptions can reinvigorate what would otherwise be an ineligible event:

- 120 days have elapsed since the complaint was reported within the company, or
- The company is impeding an investigation, or
- Action by the SEC is needed to prevent substantial injury to a company's or its investors' financial interest(s).

Finally, although not effective until August 12, 2011, the SEC rules are retroactive to tips received by the SEC after the July 21, 2010, adoption of the Wall Street Reform Act.

Are Corporate Compliance Programs Ready To Be Reformed?

Now that the dynamic has changed, it is time to refocus internal compliance programs, starting with those substantive areas where, statistically, fraud has been found more often:

- Financial statement manipulation;
- Practices made illegal by the Foreign Corrupt Practices Act, such as bribing another country's officials;
- Violations of the prohibition against illegal kickbacks — for example, payments by a hospital for illegal physician referrals; and
- Practices by a pharmaceutical manufacturer that influence decisions to prescribe a particular drug.

One study found that nearly one-quarter of fraud results in losses of more than a million dollars, that many instances of fraud are discovered by tips and that antifraud controls do help reduce it.[3]

More important perhaps are the internal processes for rooting out fraud and other conduct likely to be the subject of a disclosure to the SEC. Internal compliance programs are not only designed to discover fraud, but they also must convince employees that any attempted fraud will be discovered because the company is actually paying attention. Surprise audits and a program that encourages tips (e.g., a hotline that allows for anonymous disclosures) are important weapons in increasing vigilance and letting employees know that someone is always watching.

Equally important is a training program that teaches employees about common fraudulent activity and the ways to discover and report it. Such training should be frequently made a part of corporate newsletters or other employee outreach so that its principles are fresh in the minds of those individuals considering illegal activity. In short, a company must make it clear that fraud will not be tolerated and its employees are empowered to detect it. Anything less only invites trouble.

To ensure a top-down commitment, some companies have already established new regulatory compliance committees to "quarterback" their internal program. Those reviewing information generated by an enhanced compliance program should also have the expertise necessary to evaluate that information and the resources to seek outside expert assistance when appropriate.

Whatever the process, assigning compliance staff with a skill set adequate to assess technical information or, even more troublesome, vague disclosures, may be key to avoiding SEC involvement. Otherwise, the 120-day prohibition on certain staff members making disclosures to the SEC may be triggered.

Because those people contacted by internal investigators about known problems may still be considered an eligible whistleblower under the SEC rules, some thought should also be given to the practice of conducting internal investigations to minimize the potential for suggesting claims.

Additionally, counsel must also play a role in improving corporate compliance programs. Standard operating procedures and corporate manuals should be revisited to ensure they are consistent with the SEC rules and, just as importantly, allow a corporation to discover illegal action and address it before the SEC gets involved. After all, preventing fraud was the point of the Wall Street Reform Act.

Similarly, company marketing departments should continue to vigilantly ensure that publicly distributed marketing materials are accurate to avoid whistleblowing claims about "burying" negative information. Likewise, company policies regarding the use of social media should be adequately policed to avoid the distribution of inaccurate information. Companies can also compare their own performance to

[3] Association of Certified Fraud Examiners: "2010 Report to the Nations on Occupational Fraud and Abuse" at 4. Available at http://www.acfe.com/rttn/2010-rttn.asp.

prior years or to their competitors, to the extent such information is available, as an indicator of compliance. Outliers in the data set can be targeted for additional auditing. Finally, fraud that is discovered internally must be met with immediate and intelligent punishment. The intelligence part is crucial, given the SEC rules' anti-retaliation scheme.

Anti-Retaliation Made Paramount

Because the statute and the SEC rules include the concept of anti-retaliation, companies need to think twice about adverse employment decisions, even if justified, against complaining employees.

Retaliation includes the discharge, demotion, suspension, harassment or discrimination against a whistleblower because of his/her lawful act in providing information to the SEC. Of course, that definition promises to cause no small level of consternation for human resources personnel faced with situations where, for example, a demotion is in order notwithstanding a whistleblower's revelations.

The eligibility for anti-retaliation is determined differently from whether an individual is eligible to receive a bounty. Whereas a reward is earned for disclosures leading to the recovery of more than $1 million, there is a lesser standard with respect to retaliation. Specifically, those employees with a "reasonable belief" in the truth of their allegations are under the umbrella of the anti-retaliation protections. Moreover, employees who have been retaliated against have the right to sue in U.S. district court and can recover their counsel fees and litigation costs **and** be reinstated with double back pay.

Final Thoughts … and a Warning

Perhaps the biggest impact of the SEC rules will result from the misunderstanding of human behavior and litigation. Litigation is about leverage and maximizing pressure and thus, a financial recovery. Couple that with the normal behavior of disgruntled employees who see a dim future with a company, and these forces will combine themselves into a whistleblower claim that by its very nature is designed for maximum adverse financial impact.

Fortunately, if the SEC operates in the manner suggested by the rules, it will ask questions first and shoot later, and only if necessary. Assuming as much, corporate compliance programs should improve and complaints will be made—and kept—internally. This can increase the number of internal investigations and decrease corporate liability.

After passing through an initial period of doubts and hand–wringing, many corporations will reach the other side and find the Wall Street Reform Act had a positive impact on their organization and on the financial markets as a whole, much as Congress intended.

There is, however, a larger cost to the above-referenced benefits. Without question, the costs for implementing new compliance programs, including a method to handle whistleblower disclosures, will rise. Moreover, the incentives will be difficult for a disgruntled employee to pass up, a fact that is sure to increase complaints—and the costs of investigation.

Finally, the concept of anti-retaliation may be a factor in negotiating a resolution to enforcement actions. It may, at a minimum, require some adjustment of policies relating to the termination of disgruntled employees.

For more information about this topic, please contact David Restaino at 609.895.6701 or drestaino@foxrothschild.com.

This article previously appeared in the November 2011 issue of *Compliance Today*, a publication of the Health Care Compliance Association, and is reprinted here with permission.

Don't Take Negative Online Reviews Lying Down

By Todd A. Rodriguez

Thanks to the Internet, it is now easier than ever for unhappy patients to express their discontent for all the world to see. If you or your practice has not yet been the subject of a negative online review, there's a reasonably good chance you might be in the future. Online physician rating web sites are proliferating, and it is becoming increasingly common for disgruntled patients to vent their frustrations on the Internet. Even worse, many of these web sites permit anonymous posting, so you may not even know who your detractor is. Unfortunately, case law generally exempts rating web sites from liability provided they are only facilitating publication of the personal opinions of posters. None of this, however, means you must take a negative online review lying down. Medicine is, of course, a very personal profession, and a physician's reputation is one of his or her most valuable professional assets. Physicians should be proactive about protecting it.

Here are a few things you can do:

- First, remember the old adage that an ounce of prevention is worth a pound of cure. The best way to keep disgruntled patients from posting negative reviews online is not to have any disgruntled patients in the first place. This means in practice that physicians should treat

every patient with respect and take every patient's concerns seriously. Patients who express dissatisfaction in the office should have the opportunity to voice their concerns, and every effort should be made to try to address the issues before the patient leaves. In addition, provide customer service training for key office personnel who have direct contact with patients.

- Even providing the best customer service will not guarantee that some patients will not be unhappy with your services. It is important therefore to regularly monitor your online "image." You should routinely (at least monthly) conduct an online search of your name and your practice's name to see if comments have been posted on any web sites. Some search engines allow you to set up an "alert" to notify you by e-mail if your name appears on a web site.
- If you know who an online "poster" is, consider calling the individual and attempting to work through the concerns he or she has expressed online. If you are able to address the patient's current concerns to his or her satisfaction, see if the individual would be willing to retract the online comments.
- Consider developing a "canned" online response that you can post in reply to negative comments. The response should neither attack the poster nor admit fault. Rather it should express the practice's commitment to providing high-quality care and customer service to each patient and acknowledge that unfortunately not every patient will be happy with the circumstances or outcome of the care received.
- Review the web site's "terms of use" to see if the posting complies with them. Some web sites prohibit posters from personally naming or attacking an individual physician or claiming malpractice on the part of a physician. If you believe a posting does not conform to the terms of use, there is typically a mechanism to report the posting and often the web site will remove a noncompliant posting.
- If you have patients with positive things to say about you or your practice, encourage them to post positive comments on one or more of the available rating web sites. Not only does this counter any negative comments, but it can also push negative comments further down in the list so they are less prominent.
- Consider involving legal counsel to advise you on your options. Sometimes a well-drafted letter from an attorney to either the web site or the poster is enough to encourage them to take down the posting.

For more information about this topic, please contact Todd A. Rodriguez at 610.458.4978 or trodriguez@foxrothschild.com.

HHS/OCR Audits Are Coming: What Are Covered Entities Doing To Prepare?

By David Restaino

Those entities subject to both the HIPAA privacy and security rules should pay close attention to recent action taken by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), which will increase the frequency and depth of government audits for HIPAA/HITECH compliance over the next year. This initiative may be in direct response to some critics that OCR was not doing sufficient monitoring of compliance with HIPAA/HITECH.

Preliminary Audit Procedures

Specifically, OCR awarded a contract worth more than $9 million to KPMG, LLP for administration of the audits, which will begin shortly. The audits are required by the American Recovery and Reinvestment Act of 2009 (ARRA), which states at Section 13411, "The Secretary shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements … comply with such requirements." Details are sketchy regarding the process to identify the entities that will be audited. However, this much is known:

- The first step will be creation of audit protocols, followed by an undertaking of the actual audits.
- OCR will base its decision to audit upon risk.
- Audits will not be based upon complaints or actual reported privacy or security breaches.
- KPMG will assist OCR in establishing the program to audit covered entities and business associates and their compliance with the privacy and security rules.
- HHS staff will guide KPMG's conduct during the audits.
- The audits will include site visits, interviews with leadership, documentation, an examination of operations and an assessment of the consistency with which process is married to policy.
- Each audit will be followed by a report that will, among other things, address compliance efforts and corrective actions taken.

Who Will Be Audited?

HHS reports that every covered entity and business associate is eligible to be audited. The initial round of recipients is expected to provide a broad assessment of a complex and diverse health care industry. Thus, the audit process is designed to have OCR audit as wide a range of types and sizes of covered entities as possible. Covered individual and organizational providers of health services, health plans of all sizes and

functions and health care clearinghouses may all be considered. OCR has also made it explicitly clear that covered entities must fully cooperate with the auditors, as obligated under the HIPAA "enforcement rule." Finally, HHS reports that business associates will be included in future audits.

What Can Covered Entities Do Now To Be Ready?

For starters, they can make sure that all policies and procedures are in place now. For example, the HHS web site states that covered entities will have only 10 days to produce documents. This is not much time if policies and procedures are not already in good order.

Based on the above, the best way to get prepared is to make sure that compliance protocols are in place and being followed — today. Stated differently, all covered entities and business associates should assess their compliance efforts, ensure that timely corrective actions are taken when necessary and remain on their guard. Documentation of the proactive assessment and corrective measures should also assist in demonstrating that the compliance efforts are effective.

For more information about this topic, please contact David Restaino at 609.895.6701 or drestaino@foxrothschild.com.

This article previously appeared on the firm's HIPAA, HITECH and Health Information Technology blog (http://hipaahealthlaw.foxrothschild.com).

About the Health Law Practice

Fox Rothschild's Health Law Group comprises more than 40 attorneys who counsel clients locally, regionally and nationally. Our multioffice, multidisciplinary approach allows us to offer practical, cost-effective solutions to issues faced by longstanding stakeholders, as well as a variety of industry newcomers.

For more information about any of the articles in **Staying Well Within the Law**, please contact any member of the Fox Rothschild Health Law Practice. Visit us on the web at **www.foxrothschild.com**.

Practice Co-Chair
David S. Sokolow
215.299.2712 or 609.895.3308
dsokolow@foxrothschild.com

Practice Co-Chair
Todd A. Rodriguez
610.458.4978
trodriguez@foxrothschild.com

Newsletter Editor
William H. Maruca
412.394.5575
wmaruca@foxrothschild.com

Fox Rothschild LLP
ATTORNEYS AT LAW