AHLA

VOLUME 4 ISSUE 1 March 2015

Fraud & Abuse

A Publication of the American Health Lawyers Association
Fraud and Abuse Practice Group

Table of Contents

Chair's Column

Laura F. Laemmle-Weidenfeld
Jones Day
Washington, DC

Welcome to the Fraud and Abuse Practice Group's (F&A PG's) first newsletter of 2015. Although our PG has been very busy with a number of projects, this is our first newsletter of the 2014-2015 term. So it seems like an opportune time to introduce our PG's leadership.

This is my first year as chair of the F&A PG, although I served as a vice chair for five years leading up to this role. I assumed the chair position in late June from my predecessor, Mark A. Bonanno, who did a terrific job leading our PG for the prior three years. During his tenure, Mark ensured that the PG maintained high quality on a number of ongoing processes, such as the Advisory Opinions Task Force (Advisory Opinions TF) and the Enforcement Committee, both of which issue email alerts throughout the calendar year to our PG members. Mark's true legacy, however, is the constant emphasis on providing more value to F&A PG members. Under that mantra, we began a number of new projects during Mark's leadership, including issuing this newsletter several times a year, creating and making available online the Stark Law Toolkit, establishing a new Compliance Committee, and a number of other initiatives, the fruits of which only now are becoming visible (such as our Anti-Kickback Statute Toolkit, which is in development). I plan to continue that focus for the remaining two-and-a-half years of my term as chair.

But back to our current leadership. **Joseph M. Kahn** is new to the vice chair position this year, after serving as a lead coordinator on various projects over the last two years. He is responsible for publications, and, as such, he puts together this newsletter a couple of times a year; oversees the Enforcement Committee, the Compliance Committee, and the Advisory Opinions TF, all of which issue email alerts on relevant and timely topics throughout the year; and oversees the writing and issuance of lengthier, less time-sensitive Executive Summaries and Member Briefings.

Carol A. Poindexter is serving as a vice chair of the F&A PG for her fifth year now, and brings to her position over at strategic activities a wealth of experience with the PG as well as a strong history of innovation. In the past, whenever we needed someone to take a half-formed idea, fill it out, and run with it, Carol met the challenge. This year she will once again fill that role by working to put together a Self-Disclo-

sure Toolkit, as well as lending her capable assistance to other vice chairs who are working to develop new projects.

Heather M. O'Shea also is a veteran of our PG and is heading up membership this year. Heather helps us keep in touch with our members by tracking new volunteers (and we are blessed with many!) and helping us connect them to PG project needs, by helping us reach new categories of potential members, and by tracking and connecting with members whose membership is up for renewal or recently has lapsed. Heather also will be working with Carol to develop a protocol for continually updating our 50-State Fraud and Abuse Survey database, one of the PG's most established, and still one of the most valuable, member benefits.

This year, our PG's new vice chair of educational programs is **Kevin E. Raphael**, who, along with Joe, is a rookie vice chair but joins us after a couple of years of making significant contributions as a lead coordinator. Kevin is responsible for planning and coordinating with speakers for the PG's semi-annual luncheons at the Annual Meeting and at the Fraud and Compliance Forum—in fact, he currently is in the process of finalizing speakers for the PG's luncheon at the Annual Meeting. Kevin also is taking the lead on developing a new approach, using AHLA's new webinar platform, to creating more interactive, advance-level webinars for our PG members. For those who missed the beginner-level Bootcamp Webinar Series that the F&A PG sponsored the last few years—we will provide it again in coming years. (In the meantime, the recordings for those past webinars are now available.)

Gary W. Herschman is in his second year as a vice chair in the PG, and is responsible for research and website issues. In that role, he has primary responsibility for reviewing the new AHLA web platform and making suggestions on behalf of the F&A PG with regard to what changes and improvements would be helpful. He also is working with Carol to obtain and make available to our members more useful information about the settlements of matters under CMS' Self-Referral Disclosure Protocol.

And finally, AHLA has created a new position for the PGs and TFs this year, social media coordinator. **Alex T. Krouse** already had been assisting the PG with its Twitter committee, so we asked him to become the PG's inaugural social media coordinator. He is responsible for coordinating with the PG's other Twitter volunteers to make sure the PG maintains constant visibility on Twitter, which includes covering some of AHLA's in-person programs. Alex's and other volunteers' efforts are paying off, as evidenced by the fact that the F&A PG gained 50 more followers last month alone.

In addition to the individuals listed above, we receive tremendous support from many other volunteers, including lead coordinators and chairs and members of the various committees that provide email alerts. We could not do what we do without these individuals contributing their time and talents.

Every year when you fill out your renewal notice, you and every other member of the PG asks, "Is it really worthwhile to join the Fraud and Abuse Practice Group?" We are honored that you decided in the affirmative and have maintained your membership. Our leadership team will work hard over the remainder of the term to provide even more value for your membership fee, and to help you stay up-to-date on the ongoing developments in both compliance and enforcement in this area. Our goal is that the next time you complete your renewal notice, you ask instead, "How could I possibly justify not joining the Fraud and Abuse Practice Group?" In the meantime, if you have any comments or suggestions to help make the PG even better, please don't hesitate to stop me in the hallway at a conference or reach out to me at lweidenfeld@jonesday.com.

Sincerely,

Laura

Spilling the Beans: When a False Claims Act Defendant's Actions Trigger the FCA's Public Disclosure Bar

*Scott R. Grubman**
Chilivis Cochran Larkins & Bever LLP
Atlanta, GA

Introduction

On December 29, 2009, Robert Cunningham—a compliance officer for Calloway Laboratories—filed a False Claims Act (FCA) qui tam complaint in a Massachusetts federal district court against competing company Millennium Laboratories, alleging irregular billing practices.[1] Five days before Cunningham filed his FCA suit, Millennium sued Calloway in California Superior Court, alleging state-law claims for defamation and intentional interference with contractual relations.[2] In its Superior Court complaint, Millennium attached emails from Calloway employees to third parties suggesting fraudulent activity in Millennium's billing practices.[3] Based on this, Millennium moved to dismiss Cunningham's FCA suit, citing the FCA's public disclosure bar.[4] The Massachusetts district court agreed with Millennium and dismissed the FCA complaint.[5]

On appeal, the First Circuit made clear that a defendant's own actions can trigger the FCA's public disclosure bar:

> While we share Relator's concerns that a person or entity committing a fraud against the government could theoretically shield itself from a *qui tam* action through preemptively filing its own action, thus creating a sanitized public disclosure while barring future whistleblower action, the Supreme Court has made clear that *self-disclosure can bar such suit under the FCA*, and it has further characterized concerns about insulation from FCA liability as unwarranted in most cases.[6]

The First Circuit went on to hold that the public disclosure bar precluded some of Cunningham's allegations, but that other allegations were not disclosed in the previous suit and, therefore, not barred.[7]

In two cases from 2010 and 2011, the U.S. Supreme Court confirmed this proposition, treating as a foregone conclusion that a defendant's actions can trigger the public disclosure bar.[8]

The FCA's Public Disclosure Bar

The FCA's public disclosure bar provides:

> The court shall dismiss an action or claim under this section, unless opposed by the Government, if substantially the same allegations or transactions as alleged in the action or claim were publicly disclosed—
>
> 1. in a Federal criminal, civil or administrative hearing in which the Government or its agent is a party;
>
> 2. in a congressional, Government Accountability Office, or other Federal report, hearing, audit or investigation; or
>
> 3. from the news media,
>
> unless the action is brought by the Attorney General or the person bringing the action is the original source of the information.[9]

A relator is the "original source" of the information—and, therefore, is not prohibited from bringing suit—if the person either voluntarily disclosed the information to the government prior to the public disclosure or has knowledge that "is independent of and materially adds to" the publicly disclosed information, provided that person voluntarily provided the information to the government prior to filing.[10]

When a Defendant's Conduct Triggers the Public Disclosure Bar

As the following examples illustrate, a defendant's actions can trigger the public disclosure bar if the statutory requirements are met.[11]

Court Proceedings

The public disclosure bar provides that a qui tam action should be dismissed "if substantially the same allegations or transactions as alleged in the action or claim were publicly disclosed . . . in a *Federal* criminal, civil or administrative hearing *in which the Government or its agent is a party*."[12] Numerous courts have held that a prior public disclosure may occur through any public document available on the docket in a civil case, including a civil complaint,[13] as well as information disclosed in discovery as long as there is no court order limiting its use.[14]

The court in *Millennium* applied this provision. Importantly, the pre-2010 public disclosure bar applied in *Millennium* was broader than the current version in that the pre-2010 bar applied to public disclosures made in "a criminal, civil, or administrative hearing."[15] Under the current version of the public disclosure bar, the factual scenario present in *Millennium* would not qualify for a prior public disclosure for two reasons: first, the litigation between Millennium and Calloway was in state, and not federal, court; and second, neither the government nor its agent was a party to that litigation.[16] However, even post-amendment, where a defendant made a prior disclosure in a federal court pleading in a case in which the government or its agent was a party (for example, a prior FCA case, Medicare appeal, or bankruptcy proceeding), the public disclosure bar could be triggered.

Responses to FOIA Requests

The public disclosure bar also covers allegations or transactions publicly disclosed in a "Federal report."[17] In *Schindler Elevator Corp. v. United States ex rel. Kirk*, the U.S. Supreme Court held that responses to Freedom of Information Act (FOIA) requests are considered "reports" for purposes of the public disclosure bar.[18] Although the Court in *Schindler* applied the pre-2010 bar, which simply contained the word "report" without the word "Federal," nothing in the Court's holding suggests that it would not apply to the current version.[19] In fact, the Court in *Schindler* took an extremely broad view of the word "report" as used in the public disclosure bar; adopting Webster's Dictionary's definition: "something that gives information."[20]

Although the Court in *Schindler* dismissed concerns that a defendant might file an FOIA request to trigger the public disclosure bar, noting, among other things, that the bar would not apply if the suit was not "based upon" the initial public disclosure,[21] this safeguard no longer applies. One of the 2010 amendment's most significant changes is that the phrase "based upon" was removed from the statute, and the public disclosure bar now is triggered as long as "substantially the same allegations or transactions" alleged in the qui tam action were publicly disclosed.[22] As the Fourth Circuit has noted, though the pre-amendment version of the bar applied only where the plaintiff "actually derived" his knowledge of the fraud from the public disclosure, the post-amendment version "no longer requires actual knowledge of the public disclosure, but instead applies 'if substantially the same allegations or transactions were publicly disclosed.'"[23] Accordingly, a response to an FOIA request—even if filed by a defendant—triggers the public disclosure bar if the response contained "substantially the same allegations or transactions as alleged" in the qui tam action.

Disclosures Made Through the News Media or on the Internet

The public disclosure bar also applies to allegations or transactions publicly disclosed through the "news media."[24] Although the FCA does not define "news media," the U.S. Supreme Court has held that "[t]he 'news media' referenced in [the public disclosure bar] plainly have a broa[d] sweep."[25] Lower courts uniformly have held that "news media" include "readily accessible websites,"[26] including Wikipedia[27] and, importantly, a defendant's own publicly available website.[28] If an FCA defendant made a disclosure through the news media or on the internet, including on its own website, a subsequently filed qui tam action with substantially the same

allegations or transactions likely would be dismissed under the public disclosure bar unless the relator qualified as an original source.

Self-Disclosure to Government

The public disclosure bar applies to disclosures made in a "Federal . . . hearing, audit, or investigation."[29] In most jurisdictions, a defendant's self-disclosure to the government, without more, typically will not qualify as a "public disclosure." The First, Ninth, Tenth, and Eleventh Circuits have held that private disclosures to the government alone will not qualify as public disclosures. For example, in *Rost v. Pfizer*, the First Circuit held that disclosures by the defendant to the U.S. Department of Health and Human Services' Office of Inspector General (OIG) and the U.S. Department of Justice did not count as public disclosures for FCA purposes.[30] The court in *Rost* held:

> In our view, a "public disclosure" requires that there be some act of disclosure to the public outside of the government. The mere fact that the disclosures are contained in government files someplace, or even that the government is conducting an investigation behind the scenes, does not itself constitute public disclosure.[31]

The court in *Rost* cited the history of the public disclosure bar in support of its holding. Specifically, the court noted that, prior to the 1986 FCA amendments, the statute provided that courts had no jurisdiction over qui tam suits "based on evidence or information the Government had when the action was brought" (the "government knowledge" bar).[32] The court noted that Congress specifically eliminated the "government knowledge" bar and that permitting a private disclosure to the government to qualify as a public disclosure effectively would reinstate what Congress eliminated.[33] In jurisdictions that follow this majority rule, a defendant's self-disclosure to the government, with nothing more, will not qualify as a public disclosure.

However, the Seventh Circuit has departed from the majority rule and held that a disclosure to a public official with direct responsibilities for the allegations at issue qualifies as a public disclosure.[34] And, a few district courts outside of the Seventh Circuit, including the Southern District of New York, appear willing to follow the Seventh Circuit's minority rule.[35] In these jurisdictions, if the self-disclosure at issue is made to the appropriate public official, including through OIG's self-disclosure protocol, such disclosure might very well qualify as a public disclosure.

Why Health Care Providers Should Not Use the Public Disclosure Bar as an Offensive Weapon

Although an FCA defendant can trigger the public disclosure bar under certain circumstances, creating a public disclosure to prevent future qui tam actions would seldom—if ever—be advisable. Importantly, some of the conduct that could lead to an FCA action also could lead to criminal prosecution, including prosecution for kickbacks and certain false claims.[36] The fact that the conduct was publicly disclosed would not affect the government's ability to bring a criminal case. Moreover, because the public disclosure bar affects only qui tam actions, and not FCA actions brought directly by the government, creating a public disclosure would not even shield a potential defendant from FCA liability. [37]

And, even in the context of a qui tam action, a relator may bring suit notwithstanding a prior public disclosure if the relator qualifies as an original source.[38] Finally, conduct giving rise to FCA liability also could give rise to civil monetary penalties and exclusion.[39] For these reasons, as the U.S. Supreme Court noted in *Graham County Soil and Water Conservation District v. United States ex rel. Wilson*, "no rational entity would prepare a report that self-discloses fraud with the sole purpose of cutting of *qui tam* actions."[40]

**Scott R. Grubman may be reached at sgrubman@cclblaw.com or (404) 233-4171.*

1 *United States ex rel. Estate of Cunningham v. Millennium Labs. of Cal., Inc.*, 713 F.3d 662, 664 (1st Cir. 2013). Some of the background facts cited come from the district court's decision, which can be found at 841 F. Supp. 2d 523 (D. Mass. 2012).
2 *Id.* at 667.
3 *Id.* at 664.
4 *Id.*
5 *Id.*
6 *Id.* at 671 (emphasis added) (citing *Schindler Elevator Corp. v. United States ex rel. Kirk*, ___ U.S. __, 131 S. Ct. 1885, 1895, 179 L.E.2d 825 (2011), and *Graham Cnty. Soil & Water Conservation Dist. v. United States ex rel. Wilson*, 559 U.S. 280 (2010)).
7 *Id.* at 671.
8 *Graham County*, 559 U.S. at 300; *Schindler Elevator*, 131 S. Ct. at 1895.
9 31 U.S.C. § 3730(e)(4)(A).
10 *Id.* § 3730(e)(4)(B). The Affordable Care Act (ACA) amended the public disclosure bar in several important ways. *See generally United States ex rel. May v. Purdue Pharma L.P.*, 737 F.3d 908 (4th Cir. 2013) (discussing various changes to public disclosure bar).
11 *See supra.*
12 *Id.* § 3730(e)(4)(A)(i) (emphasis added).
13 *See, e.g., Millennium Labs.*, 713 F.3d at 670 (citing *United States ex rel. Poteet v. Bahler Med., Inc.*, 619 F.3d 104, 111 (1st Cir. 2010)); *Federal Recovery Servs., Inc. v. United States*, 72 F.3d 447, 450 (5th Cir. 1995) (quoting *United States ex rel. Siller v. Becton Dickinson & Co.*, 21 F.3d 1339, 1350 (4th Cir.), *cert. denied*, 513 U.S. 928 (1994)).
14 *United States ex rel. Stinson, Lyons, Gerlin & Bustamanta, P.A. v. Prudential Ins. Co.*, 944 F.2d 1149, 1157 (3d Cir. 1991). *Cf. United States ex rel. Kreindler & Kreindler v. United Technologies Corp.*, 985 F.2d 1148, 1157 (2d Cir. 1992); *Wang v. FMC Corp.*, 975 F.2d 1412, 1416-17 (9th Cir. 1992).
15 31 U.S.C. § 3720(e)(4)(A) (2005).
16 *See Millennium Labs.*, 713 F.3d at 669 n.5 ("In 2010, Congress amended the public disclosure provision of the FCA and explicitly narrowed the jurisdictional bar to disclosures in federal rather than federal and state cases or hearings.").
17 31 U.S.C. § 3730(e)(4)(A)(ii).
18 131 S. Ct. at 1889.

19 The addition of the word "Federal" by ACA does mean, however, that a response to a state Open Records Act request would not qualify as a public disclosure.
20 131 S. Ct. at 1891.
21 *Id.* at 1895.
22 31 U.S.C. § 3730(e)(4)(A).
23 *United States ex rel. May v. Purdue Pharma L.P.*, 737 F.3d 908, 917 (4th Cir. 2013) (internal citations omitted).
24 31 U.S.C. § 3730(e)(4)(A)(iii).
25 *Graham County*, 559 U.S. at 288; *see also Schindler Elevator*, 131 S. Ct. at 1891 ("The other sources of public disclosure in § 3730(e)(4)(A), especially 'news media,' suggest that the public disclosure bar provides 'a broa[d] sweep.'").
26 *See, e.g., United States. ex rel. Doe v. Staples, Inc.*, 932 F. Supp. 2d 34, 40 (D.D.C. 2013).
27 *United States ex rel. Brown v. Walt Disney World Co.*, 2008 WL 2561975, at * 4 (M.D. Fla. June 24, 2008).
28 *See, e.g., United States ex rel. Osheroff v. Humana, Inc.*, 2015 WL 223705, at *6 (11th Cir. Jan. 16, 2015) (holding that defendant's publicly available websites qualify as "news media" for purposes of public disclosure bar); *U.S. ex rel. Repko v. Guthrie Clinic, P.C.*, 2011 WL 3875987, at *13 (M.D. Pa. Sept. 1, 2011) (same).
29 31 U.S.C. § 3730(e)(4)(A)(ii).
30 507 F.3d 720, 728-29 (1st Cir. 2007), *overruled on other grounds by Allison Engine v. United States ex rel. Sanders*, 553 U.S. 662 (2008)).
31 *Id.* at 728.
32 *Id.* at 729.
33 *Id.* at 729-30. *See also Kennard v. Comstock Res., Inc.*, 363 F.3d 1039, 1043 (10th Cir. 2004) (holding that public disclosure requirement "clearly contemplates that the information be in the public domain in some capacity and the Government is not the equivalent of the public domain"); *United States ex rel. Williams v. NEC Corp.*, 931 F.2d 1493, 1499-1500 (11th Cir. 1991) (stating that report submitted to government officials was not a public disclosure under FCA); *United States ex rel. Meyer v. Horizon Health Corp.*, 565 F.3d 1195, 1200-01 (9th Cir. 2009). *See also United States ex rel. Whitten v. Community Health Sys., Inc.*, 575 F. Supp. 2d 1367, 1379-80 (S.D. Ga. 2008) (holding that interviews and document production during government fraud investigation did not trigger public disclosure bar); *United States ex rel. Saunders v. Unisys Corp.*, 2014 WL 1165869, at *6 (E.D. Va. Mar. 21, 2014) (holding that defendant's reports to U.S. Department of Defense OIG did not trigger public disclosure bar).
34 *United States v. Bank of Farmington*, 166 F.3d 853, 861 (7th Cir. 1999), *overruled on other grounds by Glaser v. Wound Care Consultants, Inc.*, 570 F.3d 907 (7th Cir. 2009) (holding that defendant's disclosure to a public official "who has managerial responsibility for claims being made" constitutes public disclosure).
35 In *United States ex rel. Ben-Shlush v. St. Luke's-Roosevelt Hosp.*, the district court for the Southern District of New York appears to have followed the Seventh Circuit's approach from *Bank of Farmington*, although the court concluded that even under that approach, there was no public disclosure. 2000 WL 269895, at * 2-*3 (S.D.N.Y. Mar. 10, 2000). Interestingly, despite the Tenth Circuit's holding in *Comstock, supra*, the district court for the Northern District of Oklahoma appears to have followed the Seventh Circuit's minority rule in *United States ex rel. Lancaster v. Boeing Co.*, 778 F. Supp. 2d 1231, 1244-45 (N.D. Okla. 2011) (holding that disclosure to U.S. Attorney's Office by federal law enforcement agency constituted public disclosure).
36 *See, e.g.*, 42 U.S.C. § 1320a-7b (Anti-Kickback Statute); 18 U.S.C. § 287 (criminal false claims).
37 *See, e.g., Graham County*, 559 U.S. at 300.
38 31 U.S.C. § 3730(e)(4)(B).
39 *Graham County*, 559 U.S. at 300.
40 *Id.*

Practice Groups Staff

Trinita Robinson
Vice President of Practice Groups
(202) 833-6943
trobinson@healthlawyers.org

Magdalena Wencel
Senior Manager of Practice Groups
(202) 833-0769
mwencel@healthlawyers.org

K.J. Forest
Senior Manager, Practice Groups Distance Learning
(202) 833-0782
kforest@healthlawyers.org

Brian Davis
Senior Manager, Practice Groups Communications and Publications
(202) 833-6951
bdavis@healthlawyers.org

Arnaud Gelb
Practice Groups Distance Learning Administrator
(202) 833-0761
agelb@healthlawyers.org

Crystal Taylor
Practice Groups Activities Coordinator
(202) 833-0763
ctaylor@healthlawyers.org

Dominique Sawyer
Practice Groups Distance Learning Certification Coordinator
(202) 833-0765
dsawyer@healthlawyers.org

Matthew Ausloos
Practice Groups Communications and Publications Coordinator
(202) 833-6952
mausloos@healthlawyers.org

Jasmine Santana
Practice Groups Editorial Assistant
(202) 833-6955
jsantana@healthlawyers.org

Graphic Design Staff

Mary Boutsikaris
Creative Director
(202) 833-0764
mboutsik@healthlawyers.org

Ana Tobin
Graphic Designer/Coordinator
(202) 833-0781
atobin@healthlawyers.org

Defending Against Self-Help Discovery: A Playbook

Kaitlin E. Harvie
Lisa S. Rivera
Bass Berry & Sims PLC
Nashville, TN

As the number of qui tam lawsuits continues to rise, health care companies increasingly are faced with situations in which an employee or contractor takes confidential materials from the company to pursue a lawsuit under the False Claims Act (FCA). The unique policy issues implicated by relators' conduct in pursuing FCA cases can create substantial uncertainty regarding if and how a company may recover materials protected by a confidentiality agreement or that otherwise are privileged. As a pair of recent cases has acknowledged, "courts have taken differing views" on whether confidentiality agreements are enforceable against relators in light of the strong public policy of protecting whistleblowers.[1] Given the variation among courts in addressing a relator's misappropriation of confidential materials, health care companies should be prepared to respond and understand the various tools that may help recover these materials.

FCA Trends and Self-Help Discovery

The intersection of current enforcement trends and the relevance of Protected Health Information (PHI) to FCA cases involving health care providers creates unique exposure for health care companies regarding the possibility of employees removing confidential information. In general, recent enforcement activity continues to supply ample incentive to potential whistleblowers by generating record volumes of cases brought and damages awarded to whistleblowers.[2]

At the same time, courts on one side of a current circuit split now impose more demanding standards on FCA plaintiffs by interpreting Rule 9(b) as requiring allegations of specific false claims.[3] In many cases, such as those alleging false claims based on unnecessary procedures, a relator would need to rely on PHI to develop allegations sufficient to satisfy Rule 9(b). As a practical matter, a potential relator, who in good faith pursues an FCA case against a health care company, will face challenges without access to PHI or other confidential materials. Thus, in light of recent robust qui tam activity and the practical challenges a relator faces in securing sufficient information to satisfy Rule 9(b), health care companies likely will face situations in which their confidential materials are misappropriated with increasing frequency.

Immediate Response to Learning of a Breach

A company may learn that its confidential information has been misappropriated through a variety of channels. A company may discover the breach proactively, such as through interviews in response to a compliance concern or through an audit of information systems. Frequently, however, a company may not learn that its confidential materials have been taken until years later when the company is faced with a complaint that relies on confidential information. Regardless of how a company learns that confidential materials have been taken, the company must immediately respond in a manner that maximizes claims of confidentiality or privilege and ensures compliance with any legal obligation, while also remaining mindful to avoid actions that could be perceived as retaliatory.

Preserving Confidentiality and Privileges

When faced with the unauthorized procurement of confidential materials, a company should immediately request the return of the confidential documents or data and memorialize this request. In addition, the company should consider whether it is appropriate to secure a confidentiality agreement or, if litigation already is pending between the parties, a protective order. Furthermore, an audit or investigation may be necessary to determine whether vulnerabilities in company procedures or information systems contributed to the breach, as well as to identify the scope of information taken that may not be apparent from the complaint. These measures are not only important to head off further dissemination of confidential materials; they also will enhance a company's protections against claims that it waived a privilege.[4]

Notification Requirements

Health care providers also should consider whether the breach triggers any notification requirements. For example, following a breach of unsecured PHI, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that covered entities provide notification to certain parties, including affected individuals and the Secretary of the U.S. Department of Health and Human Services.[5] Similar notification requirements apply to vendors of personal health records when a breach of unsecured information occurs.[6] Furthermore, health care providers also should consider any obligations under various state data breach laws, as almost every state has a notification statute providing for when notification is required for a breach involving personal identification information.[7]

Avoiding Risks of Retaliation Claims

Companies also must be mindful of the way in which their responses to a breach by an employee may have consequences under applicable anti-retaliation statutes. The FCA protects whistleblowers by prohibiting employers from taking adverse actions against employees who undertake "lawful acts" in furtherance of bringing a qui tam lawsuit.[8] Courts have interpreted these protections to extend to employees' actions related to investigating or collecting information about a possible fraud.[9] While an employee's removal of confidential information may provide grounds for termination under company policies or the employment agreement, disciplining an employee for the removal often will provide the employee with grounds to state a prima facie case of retaliation against the employer sufficient to survive a motion to dismiss.[10]

Compelling the Return of Documents

When an individual refuses to return confidential materials, a company may need to seek a court order to recover the materials. Typically, these scenarios arise when litigation already has been brought against the company, such that the company may attempt to recover the confidential materials through filing a counterclaim or motion for sanctions. While these options tend to succeed only when a plaintiff engages in particularly egregious conduct to obtain the confidential materials, a few courts have been willing to grant motions requesting the return of documents even when the plaintiff's conduct was less culpable.

Law Enforcement Assistance and TROs

Several options may be available to help a health care provider promptly recover confidential materials taken through self-help discovery. When confidential materials have been misappropriated through potentially criminal misconduct, a company should consider contacting law

enforcement to address the possible theft.[11] Furthermore, certain circumstances may threaten immediate and irreparable injury that would warrant the award of a Temporary Restraining Order (TRO).

Counterclaims

Depending on the nature of the confidential materials and the circumstances under which they were removed, a company may have a variety of counterclaims against the relator, such as breach of contract, conversion, or breach of fiduciary duty. In *Glynn v. Impact Science & Technology, Inc.*, a defendant company successfully filed a counterclaim against an FCA relator for breach of contract alleging the relator retained proprietary files after his termination in violation of the nondisclosure provision of his employment agreement. The district court granted summary judgment for the company on the breach of contract claim and ordered the relator to pay almost $90,000 for costs incurred by the company in recovering its confidential documents.[12]

An FCA defendant's ability to recover documents through counterclaims, however, may be limited by the strong public policy in favor of protecting whistleblowers. Some courts have refused to allow counterclaims against relators who remove documents related to a potential FCA case in violation of a confidentiality agreement.[13] Courts typically acknowledge, however, that counterclaims may be appropriate when confidential documents "[bear] no relation to [the] False Claims Act claim" and the counterclaims do not have the effect of indemnification or contribution.[14] In light of these policy concerns, a company may be unsuccessful in relying on counterclaims to recover confidential materials taken by a relator.

Motions for Sanctions

When a relator uses particularly egregious means to obtain the materials, a company may be able to recover confidential materials in connection with sanctions issued against the relator. For example, in *United States ex rel. Frazier v. IASIS Healthcare Corp.*, the district court ordered an FCA relator to return documents so that the company could adequately brief and the court could review IASIS' motion for sanctions based on the relator's misappropriation of documents covered by the attorney-client privilege.[15] Furthermore, some courts have recognized that the compelled return of documents itself may be an appropriate sanction against a party that wrongfully obtains documents outside the normal discovery process.[16] A motion for sanctions will provide means to recover documents only in limited circumstances because sanctions are appropriate only when a party engages in particularly severe misconduct, such as in blatant violation of ethical duties or by removing documents from a location to which the party clearly was not authorized access.[17]

Other Motions to Compel the Return of Documents

When an employee removes PHI for the purpose of pursing a qui tam suit under the FCA, the employee's conduct typically will not rise to a level that warrants sanctions. At least one court has been willing to compel the return of documents even when the defendant did not bring a counterclaim and the FCA relator's procurement of confidential materials was not so egregious as to constitute sanctionable conduct.

In *United States ex rel. Rector v. Bon Secours Richmond Health Corp.*, the district court ordered the return and deletion of documents and data containing PHI and trade secrets obtained by a relator from a third party who stored the materials after the relator's previous employer, a former contractor for the defendant, abandoned the materials.[18] Initially, the confidential materials did not provide the basis for the relator's claims, as the relator's counsel received the materials after the original qui tam complaint was filed. The materials did, however, help the relator add both "information about specific false claims" and additional defendants to amended complaints filed by the relator after the government declined intervention. Based on the nature of the information in the amended complaints, the defendant ultimately identified the source of the information and moved the court to order the return and deletion of the confidential materials.[19]

The court determined that the relator's actions in obtaining the documents "constitute[d] an unfair litigation tactic and a type of self-help discovery." The court acknowledged, however, that the relator's actions were "dissimilar in some ways [from] the self-help discovery" in certain cases in which a plaintiff's misconduct resulted in damages based on a counterclaim or sanctions against the plaintiff. Nevertheless, the court determined that the defendant "was likely to be prejudiced by [the relator's] self-help discovery because [the relator] possesses an indiscriminate amount of data and documents that may contain information not reachable through the discovery process" due to applicable privileges.[20] To remedy this prejudice, the court ordered the return of all documents to the defendant.[21] The court declined, however, to go so far as to impose sanctions on the relator.[22]

The *Bon Secours* decision rests on several principles that appear to be emerging from self-help discovery decisions in non-FCA contexts when a plaintiff's conduct does not provide grounds for a counterclaim or sanctions. First, sanctions are not warranted when the plaintiff has not engaged in wrongful conduct. For example, a plaintiff may have obtained materials from a third party, as in *Bon Secours*,[23] or a company's policy may not have clearly established the ownership of the materials.[24] Nevertheless, these courts have recognized that the prejudice to defendants—and potentially, third parties—requires some form of relief. Courts that provided relief in these circumstances did so in a manner "analog[ous] to [the relief afforded to] inadvertent disclosure of privileged

material" by ordering the return of original materials and precluding the use of information that would not have been discoverable or limiting its use to the current case.[25]

Conclusion

While courts have reached varying results on how a party may compel the return of confidential materials taken by a relator, health care providers should consider several practical principles in addressing the misappropriation of confidential information:

- Review company policies and procedures pertaining to confidential information to ensure expectations and restrictions are clearly communicated to employees and ownership over documents is clearly asserted. Clear protocols regarding who has access to what information will help prevent unauthorized access to the materials in the first place, as well as create a bright line of accessibility that will assist a company in establishing that the breach was unauthorized if litigation becomes necessary to recover the materials;
- Upon learning that confidential materials have been taken, immediately request the return of documents and memorialize the request;
- If the misappropriation of confidential materials is potentially criminal, consider notifying law enforcement;
- Consider whether a confidentiality agreement or protective order is necessary;
- Consider whether the breach triggers any notification requirements;
- When a current employee takes confidential materials in violation of company policies or a confidentiality agreement, ensure that the company's response to the employee minimizes the risk of implicating anti-retaliation statutes; and
- Determine whether legal action is necessary to recover the documents, and if so, what litigation mechanisms are most appropriate, including counterclaims, motions for TROs, sanctions, or other motions to compel the documents' return.

1 *Walsh v. Amerisource Bergen Corp.*, Civ. No. 11-7584, 2014 U.S. Dist. LEXIS 82064, at *2 (E.D. Pa. June 17, 2014); s*ee also United States ex rel. Notorfransesco v. Surgical Monitoring Assoc.*, Civ. No. 09-1703, 2014 U.S. Dist. LEXIS 172044 (E.D. Pa. Dec. 12, 2014).

2 *See* Press Release, Justice Department Recovers Nearly $6 Billion from False Claims Act Cases in Fiscal Year 2014 (Nov. 20, 2014).

3 *See United States ex rel. Bledsoe v. Cmty. Health Sys., Inc.*, 501 F.3d 493, 504 (6th Cir. 2007); *United States ex rel. Joseph v. Brattleboro Retreat*, No. 2:13-cv-55, 2014 U.S. Dist. LEXIS 110154, at *23-28 (D. Vt. Aug. 10, 2014).

4 *Cf. United States ex rel Schaengold v. Mem'l Health, Inc.*, No. 4:11-cv-58, 2014 U.S. Dist. LEXIS 156595, at *19-21 (S.D. Ga. Nov. 5, 2014) (defendant's failure to take "reasonable steps to rectify an inadvertent disclosure" would constitute waiver).

5 *See* 45 C.F.R. §§ 164.400-414.

6 *See* 16 C.F.R. § 318.

7 *See, e.g.*, Tenn. Code Ann. § 14-18-2107.

8 31 U.S.C. § 3730 (h)(1).

9 *See Glynn v. EDO Corp.*, 710 F.3d 209, 214 (4th Cir. 2013).

10 *See United States. ex rel. Schweizer v. Océ N.V.*, 677 F.3d 1228, 1240-41 & n.14 (D.C. Cir. 2012).

11 *See Ashman v. Solectron Corp.*, No. 08-1430, 2008 U.S. Dist. LEXIS 98934, at *4-5 (N.D. Cal. Dec. 1, 2008).

12 *See Glynn v. Impact Sci. & Tech., Inc.*, 807 F. Supp. 2d 391, 424-25, 442 (D. Md. 2011).

13 *See United States. v. Cancer Treatment Ctrs. of Am.*, 350 F. Supp. 2d 765, 774-75 (N.D. Ill. 2004).

14 *Seibert v. Gene Sec. Network, No.* 11-cv-01987, 2013 U.S. Dist. LEXIS 149145, at *25-26 (N.D. Cal. Oct. 16, 2013).

15 *See United States ex rel. Frazier v. IASIS Healthcare Corp.*, 812 F. Supp. 2d 1008, 1013 (D. Ariz. 2011).

16 *See Rollins v. Cargill, Inc.*, No. 11-1147, 2012 U.S. Dist. LEXIS 119842 (D. Kan. Aug. 24, 2012) (sanctioning plaintiff by requiring return of original versions of documents containing trade secrets).

17 *See, e.g., United States v. IASIS Healthcare Corp.*, No. 2:05-cv-766, 2012 U.S. Dist. LEXIS 6896, at *39-46 (D. Ariz. Jan. 10, 2012) (sanctioning qui tam counsel for using privileged materials taken from company by former chief compliance officer); *Fayemi v. Hambrecht & Quist, Inc.*, 174 F.R.D. 319, 325-27 (S.D.N.Y. 1997) (recognizing employee's conduct was sanctionable when he "gain[ed] access to private areas without permission or authority and copied confidential materials").

18 *United States ex rel. Rector v. Bon Secours Richmond Health Corp.*, No. 3:11-CV-38, 2014 U.S. Dist. LEXIS 1031, at *4-5 (E.D. Va. Jan. 6, 2014).

19 *Id.* at *6-10.

20 *Id.* at *18.

21 *Id.* at *19. *But see Cabotage v. Ohio Hosp. for Psychiatry*, No. 2:11-cv-50, 2012 U.S. Dist. LEXIS 105130, at*9-10 (S.D. Ohio July 27, 2012) (declining to compel return of documents containing PHI because HIPAA did not grant the court authority to do so).

22 2014 U.S. Dist. LEXIS 1031 at *18-19.

23 *Id.; G. v. Hawaii*, Civ. No. 09-00044, 2009 U.S. Dist. LEXIS 48214, at *4 (D. Haw. June 9, 2009) (order for return of documents that were "removed from [defendant's offices] by an individual without the authority to do so" when there was "no evidence that [plaintiff or counsel] acted improperly with respect to those documents").

24 *See, e.g., Bedwell v. Fish & Richardson P.C.*, No. 07-CV-0065, 2007 U.S. Dist. LEXIS 88595, at *6 (S.D. Cal. Dec. 3, 2007) (plaintiff not required to return documents when policies and procedures "[did] not conclusively establish that Defendant is the sole owner of these documents").

25 2009 U.S. Dist. LEXIS 48214, at *4; *see also Long v. Stand-By Pers., Inc.*, No. 12-CV-297, 2013 U.S. Dist. LEXIS 118528, at *5-6 (N.D. Okl. Aug. 21, 2013) (ordering return of original documents containing trade secrets and limiting use of any copies to the current case); *Eaglesmith v. Ray*, No. 2:11-cv-0098, 2012 U.S. Dist. LEXIS 60945, at *8 (E.D. Cal. May 1, 2012) (ordering return of privileged documents and subsequent production of documents in redacted form); *United States v. Comco Mgmt. Corp*, No. SACV 08-0668, 2009 U.S. Dist. LEXIS 118336, at *12-13 (C.D. Cal. Dec. 1, 2009) (ordering return of documents and precluding use of only those documents that were attorney-client communications or work product); *Lussier v. SSI Inc.*, No. 99 Civ. 5814, 2000 U.S. Dist. LEXIS 9799, at *3 (S.D.N.Y. July 17, 2000) (order for return of documents but permitting plaintiff to copy "documents for use in litigation only" when documents were discoverable).

Where Meaningful Use Meets Fraud and Abuse

Michaela D. Poizner
Baker Donelson Bearman Caldwell & Berkowitz PC
Nashville, TN

Imagine: a group of doctors, white-coated and serious-looking, sit around the moonlit fire during a scout-style campout. They take turns holding the flashlight under their faces and telling spooky stories, but these are not ghost stores—no, they are much more bone-chilling. "I opened the envelope, and it was an *audit letter*." "The agent walked in and pulled out his *badge* and said we were *under investigation*." "She said she was going to *blow the whistle*." One doctor pulls his sleeping bag over his head. Another stifles a whimper. Health care fraud enforcement is scary stuff.

The scene of terrified doctors around a campfire is more than a little far-fetched, but the idea that a regulatory compliance issue can be disastrous is not a joke. Perceived kickbacks? That will be treble damages and a corporate integrity agreement, thank you. Did not sign your personal services agreement? No reimbursement for you, and you are excluded from Medicare. Careless billers upcoding? You shall be tarred and feathered.

The provider community knows well what traditionally has called down the wrath of the government, but in the collective discussion about compliance, one program has been underrepresented: the Electronic Health Record (EHR) Incentive Program, commonly known as Meaningful Use (MU), which is mandatory for all Medicare-certified eligible providers beginning in 2015.

The Meaning(ful Use) of Life

MU may be a recent arrival to the party, but its dance card already is darn near full. More than 514,000 individual providers and hospitals are actively registered in the program, which encourages providers to incorporate the use of technology into their practices by doling out incentive payments for "meaningful use" of health information technology and docking reimbursement rates for Medicare-certified eligible providers who do not meaningfully use technology.[1] The Centers for Medicare & Medicaid Services (CMS) made the first incentive payments to providers in 2011, and, as of November 2014, providers had received more than $25 billion in incentive payments in the aggregate.[2]

MU requires providers to utilize Certified Electronic Health Record Technology (CEHRT) to meet technology-related objectives, such as recording patient demographics in an EHR and using computerized order entry for medication orders. The program is being rolled out in three stages, with each stage building on the last. Stages 1 and 2 have been implemented, and Stage 3 will begin in 2017.

There are two MU tracks: one for Medicare-certified providers and one for Medicaid-certified providers. Providers who are both Medicare- and Medicaid-certified must choose one of the tracks, but they can switch tracks one time. Under the Medicare program, incentive payments began in 2011, and the final payments will be made in 2016.[3] Beginning in 2015 and for every year thereafter (even beyond 2016), providers who are eligible to participate in the Medicare program, but do not successfully demonstrate the appropriate stage of MU, will be subject to downward Medicare payment adjustments by CMS starting at 1% and growing to 5%. The Medicaid program, which every state has implemented, also began making incentive payments to providers in 2011, but payments continue through 2021. Providers who are eligible for only the Medicaid EHR Incentive Program will not be subject to downward payment adjustments.

The Arsenal: Health Care's Big Guns

So the government is forking over billions of dollars, providers are jockeying to obtain backlogged CEHRT, and

practices are trying to completely overhaul their day-to-day operations. What could go wrong? Well, a lot. This section does not provide an exhaustive list of the potential regulatory pitfalls for MU participants, but it does review how participants could find themselves crossways with the big players in health care law: the False Claims Act (FCA), the federal Anti-Kickback Statute, and the Physician Self-Referral Law (Stark Law). This section also briefly discusses other regulatory concerns, including general fraud liability and state fraud and abuse laws.

True or False . . . Claims: The False Claims Act

The FCA prohibits "knowingly presenting (or causing to be presented) a false or fraudulent claim for payment to the federal government."[4] Unlike participating in Medicare or Medicaid, MU does not involve billing the government—so where, exactly, does MU intersect with the FCA?

First, attestations. An MU attestation is not a Medicare reimbursement claim, but a "claim for payment to the federal government," nonetheless. Providers submit attestations each year to demonstrate that they are entitled to receive EHR incentive payments (and, starting this year, to avoid reimbursement reductions). The attestation must state that the participant successfully completed *all* required measures; if the participant falls short in even one area, tough luck. The participant cannot receive even a partial incentive payment.

So, if a provider does not qualify for an incentive payment, but the attestation says that the provider does qualify, the attestation arguably is a false claim. In fact, CMS stated that it believes MU attestations are subject to the FCA.[5] And, even though we are talking about health care fraud, a false claim does not have to be submitted with any intent to defraud to violate the FCA.[6] In fact, the submitter of the claim does not even need to have actual knowledge that the claim is false—deliberate ignorance, or even reckless disregard, of the claim's truth or falsity is sufficient to constitute "knowingly."[7]

Second, overpayments. Thanks to the Fraud Enforcement and Recovery Act of 2009, failure to return an overpayment from the government is a specific example of a "reverse false claim." This means if a participant attests to MU and receives an incentive payment (or does not receive a reimbursement reduction), and subsequently realizes that it actually did not meet all of the program's criteria and thus was not entitled to the incentive payment (or should have received a reimbursement reduction), the participant arguably will be guilty of a reverse false claim if the participant does not return the payment (or excess reimbursement). And remember that mushy definition of "knowingly"? It applies here, too. So, if the participant realizes that it made a mistake in calculating patient encounters, for example, the participant cannot avoid reverse false claims liability by simply not recalculating whether it satisfied the relevant measures. We call that "deliberate ignorance," and CMS will not be impressed with your creative problem solving.

Third, coding. CMS repeatedly has expressed its concern that EHR use may result in health care fraud in the form of improper billing.[8] A letter from former U.S. Department of Health and Human Services (HHS) Secretary Kathleen Sebelius and Attorney General Eric Holder to leading industry organizations specifically raised concern about the "cloning" of patient records (copying and pasting from one record into another), upcoding as a result of using EHR systems, and the accurate billing of evaluation and management services.[9] The letter stated that the government would conduct billing audits "to identify and prevent improperly billing."[10] Based on the government's clear concern, providers should exercise caution when using EHR records as a basis for reimbursement claims to federal health care programs.

Now Accepting (CEHRT) Donations: Anti-Kickback and Stark

When you picture fraudsters luring doctors into improper referral relationships, you might think of lucrative speaking engagements in the Caribbean, lavish housing allowances, or inexplicable "bonus" payments, but do not forget a glittering new EHR system, tricked out with all the bells and whistles, in all its interoperable glory. It is enough to make a grown man misty-eyed with wonder—and, in some cases, it is enough to make doctors refer their patients straight to the gift-giver.

The reality is, CEHRT is expensive. And, in many cases, it is hard to come by. Vendors are backlogged due to providers, who are facing reporting deadline pressures, snatching up the equipment faster than it can be released. So, if you are a doctor, and a hospital says, "Let me take care of that for you," you might just say, "Thank you." And then, you might feel warm and fuzzy toward that hospital and decide that hospital really is the best place for your patients to go when they need acute care. And suddenly, you have a two-headed-monster Anti-Kickback and Stark problem.

Fortunately, CMS and the HHS Office of Inspector General (OIG) realize that, ultimately, everyone wins when doctors implement CEHRT—regardless of who pays for it. To encourage the proliferation of this technology, CMS and OIG have created an Anti-Kickback safe harbor[11] and a Stark exception[12] that protect donations of "electronic health records items and services" through 2021, provided the donations meet certain criteria:

- The donor cannot be a lab company;
- The software must be interoperable at the time the software is provided to the recipient;
- The donor cannot limit or restrict the use, compatibility, or interoperability of the items or services with other EHR systems;
- The recipient must pay 15% of the donor's cost for the donated items and services;
- The recipient cannot make the CEHRT donation a condition of doing business with the donor;

- Neither eligibility for the donation or the CEHRT's nature can be determined in a way that directly takes into account the volume or value of referrals or business generated between the parties, but the determination can be based on any other reasonable and verifiable basis, including:
  - The total number of prescriptions written by the recipient (but not the volume or value of prescriptions dispensed or paid by the donor or billed to the government);
  - The size of the recipient's medical practice;
  - The total number of hours that the recipient practices medicine;
  - The recipient's overall use of automated technology in the recipient's medical practice;
  - Whether the recipient is a member of the donor's medical staff; or
  - The level of uncompensated care the recipient provides;
- The arrangement must be set out in a written agreement covering all of the EHR items and services to be provided that is signed by the parties and that specifies the items and services being provided, the donor's cost, and the amount of the recipient's contribution;
- As far as the donor knows, the recipient cannot already have the items or services being provided;
- The donor cannot restrict the recipient's right or ability to use the items or services donated for any patient, without regard to payer status;
- The items and services donated cannot include staffing the recipient's office and cannot be used primarily to conduct personal business or business unrelated to the recipient's clinical practice or operations;
- The donor cannot shift the cost of the donated items or services to any federal health care program; and
- The arrangement cannot violate the Anti-Kickback Statute or any federal or state law governing billing or claims submission.

But Wait, There's More: Fraud Liability and State Laws

In addition to noting the caution lights flashing around the FCA, Anti-Kickback Statute, and Stark Law, MU participants should be aware of a smattering of other potential regulatory hazards.

For example, OIG has pursued criminal liability on a general fraud theory against an individual for submitting a false MU attestation. Joe White, the chief financial officer who oversaw EHR implementation for Shelby Regional Medical Center in Texas, falsely attested in 2012—using a username created for another individual and the individual's Social Security Number, without her knowledge—that the hospital satisfied the MU requirements.[13] Based on that attesta-

tion, the hospital received more than $785,000 in incentive payments in 2013.[14] A federal grand jury indicted White and charged him with making fraudulent statements to CMS and aggravated identity theft.[15] White pled guilty in November 2014 and faced up to seven years in prison, three years of probation, and a $500,000 fine.[16]

Responding to White's indictment, OIG Special Agent in Charge Mike Fields reiterated OIG's seriousness in prosecuting EHR-related fraud: "As more and more federal dollars are made available to providers to adopt Electronic Health Record systems, our office is expecting to see more cases like this one."[17]

Finally, federal health care fraud enforcement is not the only game in town: states have their own fraud and abuse (and unfair trade practices and insurance and professional misconduct) laws that MU participants should not (read: cannot) ignore. While these laws often are similar to their federal counterparts, they each have their own quirks, and MU participants should pay careful attention to how these laws may apply.

What to Do (and Not Do)

Having explored MU's potential regulatory pitfalls above (the bad news), the remainder of this article offers advice for sidestepping those pitfalls (the good news).

Fraud & Abuse Practice Group Leadership

Laura F. Laemmle-Weidenfeld, Chair
Jones Day
Washington, DC
(202) 879-3496
lweidenfeld@jonesday.com

Editorial Committee
Joseph M. Kahn, Vice Chair – Publications
Nexsen Pruet LLC
Raleigh, NC
(919) 755-1800
jkahn@nexsenpruet.com

Susan G. Kratz, Lead Coordinator
Nilan Johnson Lewis PA
Minneapolis, MN
(612) 305-7699
skratz@nilanjohnson.com

Michael E. Paulhus, Lead Coordinator
King & Spalding
Atlanta, GA
(404) 572-2860
mpaulhus@kslaw.com

Robert M. Brennan, Lead Coordinator
Parker Hudson Rainer & Dobbs LLP
Atlanta, GA
(404) 681-5969
bbrennan@phrd.com

Kevin E. Raphael, Vice Chair – Educational Programs
Pietragallo Gordon Alfano Bosick & Raspanti LLP
Philadelphia, PA
(215) 320-6200
ker@pietragallo.com

Alex T. Krouse, Social Media Coordinator
Krieg DeVault LLP
Indianapolis, IN
(574) 485-2003
akrouse@kdlegal.com

Carol A. Poindexter, Vice Chair – Strategic Activities
Norton Rose Fulbright
Washington, DC
(202) 662-4610
carol.poindexter@nortonrosefulbright.com

Gary W. Herschman, Vice Chair – Research & Website
Epstein Becker & Green PC
Newark, NJ
(973) 639-5237
gherschman@ebglaw.com

Heather M. O'Shea, Vice Chair – Membership
Jones Day
Chicago, IL
(312) 269-4009
hoshea@jonesday.com

1. **Do Not Fudge an Attestation. Ever.** This may sound obvious, but it bears repeating. Sure, missing an incentive payment by one or two numbers is frustrating, but not as frustrating as treble damages, exclusion from Medicare, and jail time.

2. **Understand What Each Measure Requires Before You Attest That You Have Met It.** The Stage 1 and Stage 2 MU Final Rules are nearly 500 pages combined. In spite of this deluge of words—or maybe because of it—aspects of the law are confusing (Do I include inpatient encounters? How quickly does a patient summary of care have to be sent?). If you are unsure whether your interpretation of a particular measure is consistent with CMS' intent, do not simply flip a coin, attest, and move forward. Seek expert counsel, and, when you do get comfortable with a particular interpretation, document how you reached your conclusion. Because when an auditor asks why you believe you have a right to an incentive payment, the auditor does not want to hear, "The coin was heads."

3. **Document and Save Everything Related to Your Attestation.** Time to channel your inner hoarder. If you ever find yourself under investigation for a false attestation, your chances of a good ending are much greater if you saved evidence supporting your attestation. Most EHR systems generate very specific reports keyed to MU measures. Pulling out the report that you ran on the date of your attestation is much more compelling during an investigation than, "I promise Mr. Investigator, this attestation is true." The FCA statute of limitations is ten years, so plan to keep your attestation support data for at least that long.[18]

4. **If You Uncover a Problem, Address It.** Say you receive an incentive payment, and later realize that you completed your attestation incorrectly, and you were not actually entitled to the payment. What are the chances you could just keep quiet, keep the money, and ride off into the sunset? Not great. Post-payment audits of EHR incentive payment recipients began in January 2013,[19] and CMS has cautioned that providers have a 1 in 20 chance of being audited.[20] It is crucial that you investigate internally to determine whether there has been an overpayment and, if so, start thinking about self-disclosure. Self-disclosure = unpleasant. Reverse false claim = really, really unpleasant. You are not an ostrich; do not stick your head in the sand.

5. **Do Not Assume Your EHR Partnership with Another Provider Falls Within the Anti-Kickback Safe Harbor and the Stark Exception.** The list of criteria for the safe harbor and exception is not short; read it carefully. This is particularly important with respect to the Stark Law, which is strict liability. An arrangement may not violate the Anti-Kickback Statute, even if the arrangement does not meet the safe harbor requirements, as long as the purpose is not to induce referrals. But the Stark Law is black and white: if you step outside the bounds of the exception, you are breaking the law. Get out your checkbook.

MU presents health care providers with the opportunity to earn valuable incentive payments while embracing technology advances that have the potential to lower costs and improve patient care. But there is no such thing as a free lunch, and the impact of fraud and abuse laws can be severe for participants who are too flippant with their attestations and their referral relationships. Providers must be savvy to the risks and take deliberate actions to stay in compliance—or risk becoming a cautionary campfire tale.

---

1 Data as of December 2014. CMS EHR Incentive Program, Active Registrations, *available at* www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/December2014_SummaryReport.pdf (last visited Feb. 26, 2015).

2 *Id.*

3 All information in this paragraph is from CMS' web page, "Medicare and Medicaid EHR Incentive Program Basics," *available at* www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Basics.html (last visited Jan. 18, 2015).

4 31 U.S.C. § 3729(a)(1)(A).

5 77 Fed. Reg. 13767 (Mar. 7, 2012).

6 31 U.S.C. § 3729(b)(1).

7 *Id.*

8 *See, e.g.*, Letter by Kathleen Sebelius and Eric H. Holder Jr. to the presidents of the American Hospital Association, Federation of American Hospitals, Association of Academic Health Centers, Association of American Medical Colleges, and National Association of Public Hospitals and Health Systems, Sept. 24, 2012, *available at* www.nytimes.com/interactive/2012/09/25/business/25medicare-doc.html?_r=2& (last visited Jan. 18, 2015).

9 *Id.*

10 *Id.*

11 42 C.F.R. § 1001.952(y).

12 42 C.F.R. § 411.357(w).

13 "Former Hospital CFO Charged with Healthcare Fraud," Press Release, Federal Bureau of Investigation, Feb. 6, 2014, *available at* www.fbi.gov/dallas/press-releases/2014/former-hospital-cfo-charged-with-health-care-fraud (last visited Jan. 19, 2015) (hereinafter, "Former Hospital CFO," Press Release).

14 *Id.*

15 Elizabeth Snell, "Former CFO Pleads Guilty in Meaningful Use Fraud," Health IT Security, Nov. 19, 2014, *available at* http://healthitsecurity.com/2014/11/19/former-cfo-pleads-guilty-meaningful-use-fraud/ (last visited Jan. 19, 2015).

16 *Id.*

17 "Former Hospital CFO," Press Release, *supra* note 13.

18 31 U.S.C. § 3731(b).

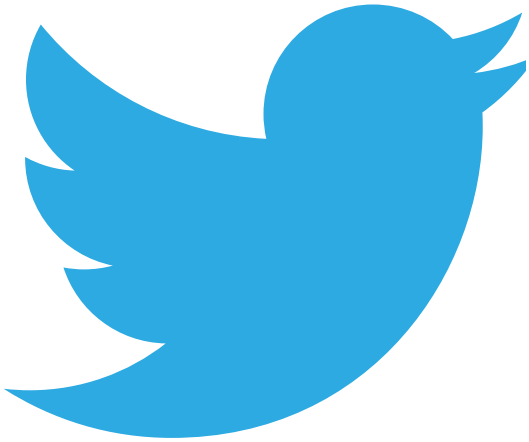
19 CMS, "EHR Incentive Programs Audits Overview," last updated Feb. 2013, *available at* www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_Audit_Overview_FactSheet.pdf (last visited Jan. 19, 2015).

20 Statistic comes from a statement by Robert Anthony, deputy director of the HIT Initiatives Group at CMS, during a telephone update of the CMS' audit efforts in April 2013, reported by Modern Healthcare, *available at* www.modernhealthcare.com/article/20130422/NEWS/304229954 (last visited Jan. 19, 2015).

F&A PG Twitter Handle Needs Volunteers

Fraud & Abuse

The Fraud & Abuse Practice Group (F&A PG) seeks attorneys to help manage its Twitter handle. F&A PG uses Twitter to increase awareness of its publications, programs, and social gatherings, and to inform PG members of breaking developments. We also alert followers to interesting discussions of fraud and abuse topics at AHLA in-person programs. Please contact Arnaud Gelb (agelb@healthlawyers.org or (202) 833-0761) if you are interested in tweeting for the F&A PG. Follow the F&A PG on Twitter @AHLA_FraudAbuse.



AHLA

1620 Eye Street, NW
6th Floor
Washington, DC 20006-4010