OBER | KALER
Attorneys at Law

Health Law Alert™

Subscribe
Reprints
PDF
Health Law Group
www.ober.com

2010 VOLUME 1

Expanded Liability Under the False Claims Act

James P. Holloway
202-326-5045
jpholloway@ober.com

The recently enacted Fraud Enforcement and Recovery Act of 2009 (FERA), Pub. L. No. 111-21, 123 Stat. 1617, included several important amendments to the False Claims Act. 31 U.S.C. §§ 3729–3733. While those amendments affect all contractors interacting with the federal government, this article focuses on the manner in which the FCA amendments are most likely to impact the health care industry. As a general matter, it is safe to declare that the amended FCA exposes health care providers to even greater potential liability for false claims than heretofore existed under the pre-FERA version of the FCA.

Liability for Retention of Overpayments

The prior version of the FCA included a so-called "reverse false claim" provision that made it unlawful to knowingly make or use a false record or statement to conceal, avoid or reduce an existing obligation to the federal government. The amended version of the FCA creates liability for any entity that "knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government." 123 Stat. at 1622 (to be codified at 31 U.S.C. § 3729(a)(1)(G)).

The amendment makes it unlawful to "knowingly conceal" an "obligation" or to "knowingly and improperly" avoid an "obligation" to pay the federal government. The definitions of key terms used in that provision broaden the scope of the FCA in a way that has a significant impact on providers. The statute defines an *obligation* as "an established duty, whether or not fixed, arising from an express or implied contractual, grantor-grantee, or licensor-licensee relationship, from a fee-based or similar relationship, from statute or regulation, or *from the retention of any overpayment.*" 123 Stat. at 1623 (to be codified at 31 U.S.C. § 3729(b)(3)) (emphasis added). The statute defines knowingly as "actual knowledge" of false information, or "deliberate ignorance" or "reckless disregard" as to the truth or falsity of information. 123 Stat. at 1622 (to be codified at 31 U.S.C. § 3729(b)(1)). Those definitions are subject to differing interpretations, and the statute does not attempt to define what constitutes "improperly" avoiding a repayment to the government.

The legislative history of the FCA amendment suggests that providers have a limited window of time to return an overpayment without creating FCA liability:

In this Issue

OBER | KALER
Attorneys at Law

Health Law Alert™

Subscribe
Reprints
PDF
Health Law Group
www.ober.com

2010 VOLUME 1

In this Issue

New York Medicaid Makes Compliance Program Mandatory

William T. Mathias
410-347-7667
wtmathias@ober.com

Did you have $500,000 in revenues from NY Medicaid in the past 12 months?

If the answer is yes, you were required to have a compliance program in effect as of October 1st and must submit a signed certification by December 1st.

Earlier this year, the New York State Office of the Medicaid Inspector General (OMIG) adopted final regulations requiring compliance programs for individuals and entities that either order from the NY Medicaid program, submit claims on behalf of themselves or others, expect to claim, or expect to receive $500,000 or more in NY Medicaid funds in any 12-month period. NY is the first state Medicaid program to make compliance programs mandatory. The regulations require that a compliance program include:

- A written code of conduct or code of ethics for employees and others;
- Designation of an employee vested with responsibility for the day-to-day operation of the compliance program;
- Training and education of all affected employees and persons associated with the provider including governing body members;
- A mechanism for communicating and reporting compliance issues, including a method for anonymous and confidential reporting;
- Disciplinary policies to encourage good faith participation in the compliance program;
- A system for routine identification of compliance risk areas specific to the provider type;
- Systems for responding to compliance issues, investigating potential compliance problems, and correcting problems; methods to implement procedures, policies and systems to reduce the potential for reoccurrence; identifying and reporting compliance issues to OMIG; and refunding overpayments; and

- A policy of non-intimidation and non-retaliation for good faith participation in the compliance program.

While these requirements are similar to the requirements under the federal sentencing guidelines and various OIG compliance guidance, the mandatory nature of these requirements puts added emphasis on the need to have an effective compliance program that meets all of the requirements.

Each December 1st, providers will be required to submit a signed certification to OMIG that they have a compliance program in place that meets the requirements. OMIG has posted the certification form on its website and recommends that it be signed by a member of senior management or a member of the provider's governing body. Providers who do not have a satisfactory compliance program or do not submit the signed certification form may be subject to sanctions and penalties, including revocation of their Medicaid participation agreement.

*Additional information about the New York requirements can be found on the OMIG website at **www.omig.state.ny.us/data/content/view/81/65**/ or by contacting **Bill Mathias**.*

OBER | KALER
Attorneys at Law

Health Law Alert™

Subscribe
Reprints
PDF
Health Law Group
www.ober.com

2010 VOLUME 1

Arkansas Court Enjoins Hospital's Use of Economic Credentialing Policy

John J. Eller*
410-347-732
jjeller@ober.com

Earlier this year, an Arkansas trial court issued a permanent injunction enjoining a nonprofit hospital, Baptist Health, from enforcing its economic credentialing policy. The policy mandated the denial of staff privileges to any physician who, through himself or his immediate family member "directly or indirectly, acquires or holds an ownership or investment interest in a competing hospital." *Baptist Health v. Murphy*, 365 Ark. 115, 118 226 S.W.3d 800, 805 (2006), *remanded to* No. CV 2004-2002 (Feb. 27, 2009) (order granting permanent injunction).

Baptist Health enforced its policy against a group of cardiologists, who, through membership in Little Rock Cardiology Clinic, held a 14.5 percent interest in a competing private acute care cardiology hospital, Arkansas Heart Hospital. The physicians subsequently sued the hospital alleging, among other claims, that the policy violated the federal antikickback statute and the Arkansas Deceptive Trade Practices Act, and that the policy tortiously interfered with the physicians' contractual relationship with their patients. The trial court issued a preliminary injunction, and defendants appealed. The Supreme Court granted certiorari, bypassing the intermediate court, and remanded the case back to the trial court for further findings of fact. Once again, the trial court issued a preliminary injunction and the defendants appealed. The Arkansas Supreme Court affirmed the trial court's grant of the preliminary injunction but invalidated the physicians' antikickback claim because the policy did not discourage the physicians from referring patients to hospitals other than Baptist Health.

The trial court concluded the case by issuing a permanent injunction enjoining the defendants from denying staff membership and privileges to the plaintiffs. In so doing, the court found that Baptist Health's policy tortiously interfered with the relationship of the physicians and their patients. *Baptist Health v. Murphy*, No. CV 2004-2002 (Feb. 27, 2009). The court held that a contractual relationship existed between the physicians and their patients and that the hospital knowingly and intentionally interfered with that relationship. The court deemed the economic credentialing policy "improper" because the policy contravened public policy and was overbroad in its scope. The court found public policy disfavors economic credentialing because economic

In this Issue

credentialing punishes physician investment in specialty hospitals, which reduces diversity in the health care market. The court found invalid the hospital's arguments that the policy was necessary to protect its financial viability, because the hospital failed to specifically prove the physician conflicts of interest impacted the hospital's $30 to $40 million annual profits. In addition, the court used this evidence to buttress its findings that the hospital had an anti-competitive purpose in promulgating the policy, rather than an intent to protect its capability of serving the community. Next, the court found that the hospital's historical inability to fulfill the community's need for available cardiology beds justified the court in enjoining use of a policy that may reduce the number of available beds.

The court next held that, because it contravened public policy, the economic credentialing policy violated the Arkansas Deceptive Trade Act. In reaching this conclusion, the court hypothesized that Baptist Health's enforcement of a policy that contravened the public's interest could compromise its 501(c)(3) tax-exempt status.

The hospital unsuccessfully tried to persuade the court to follow a factually similar case, *Walborn v. UHHS/CSAHS-Cuyahoga, Inc.*, No. CV-02-479572 (Ct. Common Pleas, Cuyahoga Cnty. June 16, 2003), in which the court upheld the hospital's economic credentialing policy. The Arkansas court distinguished *Walborn*, in which the hospital gave physicians an opportunity to challenge economic credentialing decisions via a hearing. No such right was afforded under Baptist Health's policy. Also, in *Walborn*, the court found the economic credentialing policy was necessary to protect the hospital's continued viability.

Throughout its decision, the *Baptist Health* court emphasized the importance of the physician-patient relationship, both as an essential source of referrals and revenue for the physician, as well as a means to providing the continuity of care that improves patient outcomes. The court suggested that, unless a hospital can demonstrate a valid justification for interfering with the physician-patient relationship, public policy will protect it.

Ober|Kaler's Comments

Economic credentialing began as a hospital's consideration of limited economic criteria, e.g., physician overutilization of costly services, in a context that usually related economic factors to quality of care and/or professional competence. Over time, there has been a growing emphasis on purely economic criteria. Economic credentialing has evolved into a hospital's consideration of a broad array of economic criteria, including such factors as those involved in *Baptist Health*. The *Baptist Health* decision is among the minority of economic credentialing cases finding for the physician-plaintiffs. Most federal courts uphold economic credentialing policies when challenged under federal antitrust law. Similarly, most state courts uphold those policies when challenged under state law claims.

Baptist Health may appear to be a victory for opponents of economic credentialing policies. However, one may also fairly conclude that the court did not find the hospital's economic credentialing policy inherently defective. Rather, the court enjoined the hospital from enforcing its policy because the hospital failed to provide evidence to demonstrate adequate justification for an economic credentialing policy consistent with public policy considerations. The hospital's case primarily provided post hoc justifications for the policy. It appears that had there been different factual underpinnings at the hospital for the same policy, the court could have ruled in favor of the hospital. If an economic credentialing policy is appropriately developed, justified and implemented, it is more likely to withstand scrutiny. If it is not, it may be successfully challenged.

*Mr. Eller would like to thank Delia Stubbs for her contributions to this article.

OBER | KALER
Attorneys at Law

Health Law Alert™

Subscribe
Reprints
PDF
Health Law Group
www.ober.com

2010 VOLUME 1

HITECH Act Breach Notification Rule Now in Effect, But No Sanctions Apply Until 2010

James B. Wieland
410-347-7397
jbwieland@ober.com

The HHS Office for Civil Rights (the OCR) published its interim final rule for Breach Notification for Unsecured Protected Health Information, implementing section 13402 of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), in the Federal Register on August 24, 2009. 74 Fed. Reg. 42,740 (Aug. 24, 2009). As an interim final rule, the regulation is subject to a 60-day comment period, and comments received may result in further changes or clarifications. Highlights of the PHI Breach Notification Rule and the OCR's comments and analysis that accompanied it are discussed below. *[For a more complete overview of the HITECH Act itself, including the statutory provisions governing breach notification, see* ***"The Health Information Technology for Economic and Clinical Health Act: Congress Includes Sweeping Expansion of HIPAA and Data Breach Notification Requirements in the Stimulus Bill,"*** *which appeared in Ober|Kaler's* Healthcare Information Privacy, Security and Technology Bulletin.]

The HITECH Act requires notification to individuals in the event of a breach of the security or the privacy of unsecured protected health information. Unsecured protected health information is defined in the Act as protected health information that is not secured through a technology or methodology specified in guidance by HHS. Such guidance was published in the *Federal Register* on April 27, 2009, and is supplemented in a companion portion of the August 24, 2009, PHI Breach Notification Rule. According to the guidance, electronic protected health information can be secured by encryption. Paper protected health information can be secured by destruction. No means are described for securing oral protected health information within the meaning of the HITECH Act.

Under the Act, business associates are required to provide notification of a breach to covered entities and covered entities are required to provide the notification to the affected individuals and to HHS.

Effective Date and Delay of Sanctions

In this Issue

Summary

Under the HITECH Act, the breach notification requirements become effective 30 days after publication in the Federal Register. The OCR followed the letter of the Act in this respect: "Compliance is required for breaches occurring on or after 30 calendar days from the publication of this rule." 74 Fed. Reg. 42,756. However, referring to the concerns of covered entities and business associates about the difficulty of achieving compliance within the mandated 30 days and citing some ambiguity within the HITECH Act, the OCR went on to state:

[W]e will use our enforcement discretion to not impose sanctions for failure to provide the required notifications for breaches that are discovered before 180 calendar days from publication of this rule. . . . During this initial time period — after this rule has taken effect but before we are imposing sanctions — we expect covered entities to comply with this subpart and will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance.

74 Fed. Reg. 42,756–57.

Comment

Realistically, this suspension of the imposition of sanctions gives covered entities and business associates some welcome breathing room to complete putting the protocols for compliance into effect. However, covered entities and business associates still must provide notification of breaches, starting 30 days after publication of the PHI Breach Notification Rule. The OCR specifically noted that covered entities and business associates should already have breach notification procedures in place to comply with state consumer protection laws requiring notification to individuals of the compromise of the security of identity theft-related information including, in California, medical information. Further, as discussed below, the OCR takes a firm line in the PHI Breach Notification Rule as to when a breach is deemed discovered for the purpose of the notification requirement. Covered entities and business associates who fail to determine the date of deemed discovery of a breach, especially towards the end of the interim period, may be vulnerable to sanctions.

Unauthorized Acquisition, Access, Use or Disclosure

Summary

A breach under the HITECH Act is the "unauthorized acquisition, access, use, or disclosure of protected health information." The PHI Breach Notification Rule clarifies that an unauthorized access or use is one that is not permitted under the HIPAA Privacy Rule. Significantly, this leads the OCR to note that "uses or disclosures that impermissibly involve more than the minimum necessary information . . . may qualify as breaches. . . ." 74 Fed. Reg. at 42,744. The OCR reminds covered entities and business associates that the breach notification requirement applies to protected health information in written, electronic, or oral form.

Comment

This is one of several indications in the PHI Breach Notification Rule of the significance of guidance that will be issued in accordance with section 13405 (b) of the HITECH Act dealing with the "minimum necessary" requirements of the Privacy Rule. Covered entities must use and disclose only the minimum necessary amount of protected health information needed for a particular situation, subject to exceptions for treatment-related disclosures and several other purposes. Pending issuance of minimum-necessary guidance, section 13405 (b) of the HITECH Act mandated use of a limited data set "to the extent practicable." While predicting the content of future guidance is not possible,

covered entities and business associates should consider the suitability of the limited data set for non-treatment-related disclosures of protected health information. The minimum-necessary guidance is due not later than 18 months after enactment of the HITECH Act, that is, on or before August 17, 2010. The limited data set and its role under the breach notification provisions of the HITECH Act are discussed further below.

Compromises of the Security or Privacy of Protected Health Information

Summary

While the HITECH Act simply states that a breach is a use or disclosure which "compromises the security or privacy" of protected health information, the PHI Breach Notification Rule provides important clarification that will help covered entities and business associates make notification decisions by articulating a "harm threshold" for a determination that security or privacy has been compromised. For there to have been a compromise requiring notification of subject individuals, a breach must be one that "poses a significant risk of financial, reputational, or other harm to the individual." 74 Fed. Reg. at 42,744. Covered entities and business associates are advised to perform a risk assessment, and the OCR makes it clear that documentation of that risk assessment will be key if notification is not given.

In discussing the risk assessment, the OCR articulates five factors to be considered.

- The first factor is the regulatory status of the person or entity that impermissibly used protected health information or to whom the protected health information was impermissibly disclosed. The OCR indicates that disclosure to a HIPAA covered entity or to an agency that is governed by another federal privacy law may not pass the harm threshold, since the recipient is obligated to protect the information.

- The second factor is the nature of the mitigation efforts that were undertaken. The OCR indicates that immediate and effective steps, such as promptly obtaining assurance from the recipient that the information will not be further used or disclosed (such as through a confidentiality agreement) or will be destroyed may make the possibility of harm less than significant.

- For the third factor, the OCR states that if impermissibly disclosed protected health information is promptly returned without being accessed for an improper purpose, the possibility of harm may not be significant. The example given is of a lost or stolen laptop, which is recovered with a forensic analysis showing that information was not opened, transferred, or otherwise compromised.

- The fourth factor identified by the OCR is the type and amount of protected health information involved in the impermissible use or disclosure. The name of an individual and the fact that the individual received services from a hospital may not pass the significant risk threshold; the name of the individual and the fact that the individual received services that may be associated with a particular medical condition (cancer is the example given) or from a specialized type of provider (a substance abuse program is the example given) may.

- Finally, the OCR provides a fifth factor to be considered if the breach involves a limited data set. Under the Privacy Rule, a limited data set is protected health information from which all 16 direct identifiers (e.g., name and address) have been removed. However, the limited data set is still protected health information since it is capable of re-association

with the subject individual through use of other data. The OCR stated that, in assessing the harm threshold for a breach involving a limited data set, the likelihood of re-association with the individual is a factor to be considered. In addition, the OCR enacted a specific exception from the breach notification requirements for a limited data set that, in addition to excluding the 16 direct identifiers, also excludes date of birth and zip code of the subject individual. This factor applies regardless of whether the limited data set was assembled for one of the purposes permitted under the Privacy Rule, such as research. The OCR specifically invited comments on this limited exception.

Comment

Taken together, the OCR's examples provide clarity and some comfort for covered entities and business associates dealing with a number of recurring situations. A medical bill sent to the wrong address but promptly returned unopened; a laptop left at a meeting which was promptly recovered with an event log that shows it was not powered up during the time it was missing; a patient file mistakenly sent to the wrong physician's office – each of these may fail to meet the OCR's harm threshold and not require notification of subject individuals. The specific examples also provide a useful basis for judging analogous situations.

The specific exemption afforded by the OCR for a limited data set which also lacks date of birth and zip code information, the latter two being data that is useful for probabilistic matching, a common technique for re-identification of a limited data set through comparison with other available data, may have significance in connection with the August 2010 minimum-necessary guidance. This type of "enhanced limited data set" may represent one potential standard for minimum necessary uses and disclosures, at least certain purposes.

Exceptions to Breach

Summary

The HITECH Act contains three statutory exceptions to the definition of a breach. In the PHI Breach Notification Rule, the OCR provides examples to flesh out each of these exceptions.

- As to the first exception, unintentional, good faith acquisition, access or use by an employee or other individual acting under the covered entity's or business associate's authority when there is no further use or disclosure, the OCR expands the term employee to include members of the covered entity's or business associate's work-force, a term defined in the Privacy Rule to include, for example, unpaid volunteers working in a covered entity. The OCR illustrates its interpretation of this exception with the example of a billing employee opening an email transmitted to him in error, who notices the error, alerts the sender and deletes the email. By contrast, the OCR cites a work-force member who looks through patient records for information about a friend's treatment, as a violation.

- The second statutory exception covers inadvertent disclosures by one individual authorized to access protected health information to another individual within the same facility who is also authorized to access protected health information, if the information is not further disclosed. Here, the OCR expands the definition of facility to specifically include covered entities established under HIPAA as an organized health care arrangement (such a hospital and members of its medical staff, if they collectively meet the standards for an OHCA set forth in the Privacy Rule) and similarly situated individuals to mean individuals within the same organization who are authorized to access protected health

information, even if the two individuals do not have the same type or scope of rights to access protected health information. Finally, the OCR states that the same facility includes all the facilities of a covered entity, such as a hospital system with multiple locations.

- The third and broadest exception set forth in the HITECH Act applies to an unauthorized disclosure of protected health information to a person who would not reasonably have been able to retain the information. The OCR gives the example of a covered entity sending a number of Explanation of Benefits to the wrong addresses "due to a lack of reasonable safeguards." Those EOBs that are returned unopened as undeliverable do not constitute a breach of the privacy or security of the EOB information. A nurse who, after mistakenly handing discharge papers to the wrong patient and promptly recovering them, forms a reasonable conclusion that the recipient could not have read or otherwise retained the protected health information in the papers, also does not cause a breach, according to the OCR.

Comment

The examples provided by the OCR are useful and deal, directly or by analogy, with many recurring situations that covered entities and business associates feared would require breach notification, based on the plain language of the HITECH Act. Covered entities with large scale or geographically distributed operations may wish to develop protocols for taking advantage of the clarity these examples provide, as appropriate to the covered entity's or business associate's own situation, so that "minor" incidents can be quickly documented, if not actually resolved, at the local level, limiting the demands on the organization's privacy officer or other responsible individual as to recurring situations that, given the OCR's examples, do not require notice. The burden of proof is, of course, on the covered entity or business associate. Clear and detailed documentation prepared at or near the time of the incident will be important.

Notification to Individuals

Summary

The HITECH Act provides that the time period for notification of individuals starts when the covered entity, in the exercise of reasonable diligence, should have known of the breach. Notice can be imputed to the covered entity from a variety of its representatives, including employees (other than the employee causing the breach) and from agents.

Notification must be provided without unreasonable delay and in no event later than 60 calendar days after the breach is known or deemed known by attribution. The OCR defines *reasonable diligence* as "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances." 74 Fed. Reg. at 42,749. The OCR's comments make it clear that the 60-day period is not tolled by the time spent in analysis or investigation: "Thus, the time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in this rule." 74 Fed. Reg. at 42,749.

While the HITECH Act requires business associates to notify the covered entity of a breach, the OCR states that the knowledge of a business associate can be imputed to the covered entity, without the mandated notice, if the business associate is an agent of the covered entity. The OCR also explicitly affirms what is implicit in the HITECH Act, that the 60-day period is the outside limit and circumstances may well make waiting the full 60 days unreasonable and a violation of the law.

In discussing the content of the notice to individuals, the OCR specifies that

the notice should not include protected health information or other sensitive information. The OCR states that, rather than describing steps to "mitigate loss" (the term used in the HITECH Act), the notice must describe the steps being taken to "mitigate harm to the individual." In an aside, the OCR adds that the harm to be mitigated "is not limited to economic loss." 74 Fed. Reg. at 42,750.

Plain language should be utilized in the notice. The OCR states that other statutory accommodations under laws such as the Americans with Disabilities Act (Braille, large print, or audit) must be available. The PHI Breach Notification Rule contains extensive discussion of the mechanics of notice to minors or to representatives of deceased individuals as well as of the use of substitute notice when current mailing (or email, if the individual has consented to email notice) addresses are not available. In certain circumstances, telephone notice to an individual may be left on an answering machine, according to the OCR; however, that notice should be limited to the covered entity's name, contact phone number and the fact that the covered entity has "a very important message" for the individual. The PHI Breach Notification Rule also includes discussion of media notice, web posting and notification to the Secretary, as required in specific circumstances described in the HITECH Act.

Comment

This section of the PHI Breach Notification Rule contains useful and detailed discussion of the mechanics and nuances of providing the various types of notification required by the HITECH Act. It also provides guidance to covered entities and business associates about avoiding duplicate notices to individuals arising from the same event, a clearly articulated goal of the OCR.

Notification by a Business Associate

Summary

The OCR states that if the protected health information subject to a business associate's breach cannot be attributed to a single covered entity or set of covered entities for which the business associate provides a function or activity, then all potentially affected covered entities must be notified, presumably so that some means of attribution can then be devised by the parties. Covered entities and business associates are free, according to the OCR, to determine who should receive the notice within the covered entity's management structure.

One of the most significant provisions in the OCR's discussion of a business associate's role in the breach detection and notification process concerns the circumstances in which the business associate will be deemed an "agent" of the covered entity, and therefore within the language of the HITECH Act for purposes of imputing the business associate's knowledge of a breach to a covered entity. The OCR applies the "federal common law of agency" to the determination of a business associate's status. If a business associate is an agent, knowledge will be imputed to the covered entity; if a business associate is an independent contractor, knowledge will not be imputed (at least not automatically).

The HITECH Act obligates the business associate to provide certain information to the covered entity that is necessary for the notice. The OCR modifies this in the PHI Breach Notification Rule, by adding the qualifier "to the extent possible" to the language describing the business associate's obligation. The OCR makes it clear that notice to the covered entity should be provided as soon as the business associate is aware of the breach, even if the business associate's investigation is continuing. An example provided by the OCR indicates that some of the burden may, in appropriate circumstances, shift to the covered entity; a record storage company holding "hundreds of boxes" of medical records discovers several boxes are missing and cannot

identify the individuals whose records were in the boxes. In this situation, the OCR states: “It is not our intent that the business associate delay notification of the breach to the covered entity, when the covered entity may be better able to indentify the individuals affected.” 74 Fed. Reg. at 42,754. The PHI Breach Notification Rule provides that the business associate must provide the covered entity with any other information that the covered entity is required to include in the notice, either at the time the business associate provides notice to the covered entity or later.

The OCR concludes its discussion of the HIPAA requirements as to breach notification between covered entities and business associates with a paragraph that stresses the freedom of the parties to contractually allocate responsibilities, so long as the requirements of the PHI Breach Notification Rule are met. This flexibility includes not only when the notification from the business associate

is required but also which party will provide notice to individuals. The OCR states, “We encourage the parties to consider which entity is in the best position to provide notice to the individual, which may depend on circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.” 74 Fed. Reg. 42,755. The parties are also encouraged to ensure that the individual receives only a single notification of the breach, a point repeated by the OCR in the PHI Breach Notification Rule.

Comment

While the provisions of the HITECH Act are relatively straightforward – if a business associate discovers a breach related to the protected health information of a covered entity, the business associate must notify the covered entity and the covered entity must provide the notification to individuals required by the HITECH Act – the mechanics of implementation are likely to be more complicated, as reflected in the OCR’s discussion of the issue.

The OCR indicates, and common sense supports, negotiation of specific allocations of breach notification responsibility between the parties to a business associate agreement, within the parameters of the HITECH Act. The OCR indicates a significant degree of flexibility; while the act contemplates notice to individuals by the covered entity, the OCR, in language quoted above, appears to authorize that burden to be shifted to the business associate in appropriate circumstances.

The status of a business associate as an agent or as an independent contractor has significant consequences in terms of the deemed date of discovery of a breach by a covered entity. The OCR’s test for agency status is the federal common law, which, while not always as well-fleshed-out as state law, is typically used in federal regulations to ensure national uniformity. The Restatements of Law have been referred to as a source of federal common law, in the absence of any more specific authority. This business associate’s status as an agent may be influenced by language in the business associate agreement or in the underlying service arrangement, depending on the circumstances. This and other provisions of the HITECH Act mean that covered entities and business associates should be alert to situations in which a “standard” business associate agreement may not be in the best interests of the parties, and negotiate accordingly.

This review of the Interim Final Rule for Breach Notification for Unsecured Protected Health Information is for the purpose of information and to alert entities and their advisors that are potentially affected by the rule to its general content. It covers the points deemed by the author to be of the most interest, not every point raised in the rule. This article does not constitute legal advice to any specific entity or as to any individual situation.

Mr. Wieland is a principal in the Health Law Group at Ober|Kaler. He heads the firm's Health Care Information Privacy, Security and Technology practice.

OBER | KALER
Attorneys at Law

Health Law Alert™

Subscribe
Reprints
PDF
Health Law Group
www.ober.com

2010 VOLUME 1

Unfiled Discovery Documents in Contract Action Not Public Disclosure Under FCA

Chelsea S. Rice
202-326-5030
csrice@ober.com

On May 12, 2009, the United States District Court for the Southern District of Ohio, Western Division, denied a motion to dismiss an FCA *qui tam* action after finding that unfiled discovery materials in a prior breach of contract case did not constitute a public disclosure that would bar the relator from bringing his claim under the FCA. U.S. ex rel. *Fry v. Health Alliance of Greater Cincinnati*, No. 1:03-cv-00167 (S.D. Ohio May 12, 2009).

Factual Background

On March 7, 2003, the relator, Dr. Harry F. Fry, filed a *qui tam* complaint against defendants The Christ Hospital and Health Alliance of Greater Cincinnati (hereinafter, "the defendants") for allegedly engaging in a "pay-to-play" scheme that violated federal fraud and abuse laws. The government elected to intervene on April 1, 2008. The defendants sought to dismiss the relator from the action, based on the grounds that his complaint was premised on disclosures in previous litigation, thus barring him under the FCA's "public disclosure bar."

The documents at issue were discovery documents from a previous breach of contract action between Medical Diagnostic Associates and University Internal Medicine Associates, Inc. — documents upon which certain allegations in the relator's *qui tam* complaint were based. The relator argued that only documents filed with the court (i.e., the complaint) constitute a public disclosure for purposes of the FCA, not documents exchanged between private parties as part of discovery.

Legal Analysis

In reaching a decision on the motion to dismiss, the court was called on to interpret a recent Sixth Circuit decision, *U.S. ex rel. Poteet,* 552 F.3d 503 (6th Cir. 2009). In *Poteet*, the Sixth Circuit held that for a relator's *qui tam* action to be barred by a prior public disclosure of the underlying fraud, "the disclosure must have (1) been public, and (2) revealed the same kind of fraudulent activity against the government as alleged by the relator." *Id*. at 511. The Sixth Circuit went on to clarify that a public disclosure "includes documents that

In this Issue

have been filed with a court, such as discovery documents, and a plaintiff's complaint." *Id*. at 512.

The defendants argued that *Poteet* did not decide the issue of whether unfiled discovery could constitute public disclosure under the FCA. However, the court agreed with the government's contention that if unfiled discovery in litigation could constitute public disclosure it would remove incentives for relators to blow the whistle on fraud. In addition, the government "plainly stated" that it relied on the relator's information and without it the government would have had no knowledge of the case.

The court found that *Poteet*, by stating that publicly filed documents amount to a public disclosure, necessarily excluded unfiled documents from the public disclosure bar. The court also said that there are a number of policy reasons for such a rule: "[T]he whole purpose of the FCA is to harness incentives for a whistleblower or 'private attorney general' to report to the government alleged fraud that otherwise could go undiscovered." *Fry* at pp. 6–7.

The court noted that there may be instances in which unfiled discovery documents may be disclosed through other avenues, implying that those situations may constitute "public disclosure" for purposes of the FCA. However, in this case, the discovery documents did not preclude the relator from bringing his *qui tam* claims, and thus the court denied the defendant's motion to dismiss. The court also rejected the defendant's suggestion that the public disclosure issue would be appropriate for immediate appellate review, finding that such an appeal would not materially advance the termination of the litigation.

OBER | KALER
Attorneys at Law

Health Law Alert™

Subscribe
Reprints
PDF
Health Law Group
www.ober.com

2010 VOLUME 1

Supreme Court: Appeal Deadline Applies in FCA Action Even If Government Has Not Intervened

Chelsea S. Rice
202-326-5030
csrice@ober.com

The Supreme Court issued a unanimous decision on June 8, 2009, holding that when the United States has declined to intervene in a privately initiated FCA action, it is not a "party" to the litigation; thus, the 30-day time limit for filing a notice of appeal applies. *U.S. ex. rel. Eisenstein v. City of New York*, 129 S.Ct. 2230 (2009), 556 U.S. ___ (2009).

Factual and Procedural Background

The petitioner (plaintiffs Eisenstein and four other New York City employees) filed a *qui tam* action in the name of the United States against respondent City of New York and several of its officials, challenging a fee charged by the City to nonresident workers. According to the plaintiffs, the fee violated the FCA by depriving the United States of tax revenue that it otherwise would have received if the fee had not been deducted from the workers' taxable income.

The government declined to intervene in the action and the district court subsequently granted the defendants' motion to dismiss the complaint, entering a final judgment in their favor. The petitioner filed a notice of appeal 54 days later. While the appeal was pending, the Second Circuit Court of Appeals *sua sponte* ordered the parties to brief the issue of whether the notice of appeal had been timely filed.

Federal Rule of Appellate Procedure 4(a)(1)(A)-(B) and 28 U.S.C. §§ 2107(a)-(b) generally require that a notice of appeal be filed within 30 days of the entry of judgment, but extend the period to 60 days when the United States is a party. The petitioner argued that the appeal was timely because it was filed under the 60-day limit because the United States is a party to every FCA suit. The respondents countered that the appeal was untimely under the 30-day limit because the United States is not a party to an FCA action absent formal intervention or other significant participation. The Second Circuit agreed with the respondents and dismissed the appeal as untimely. The Supreme Court granted certiorari to resolve a split among the circuits on this issue.

In this Issue

The Supreme Court's Holding

Writing on behalf of a unanimous Court, Justice Clarence Thomas explained that while the United States is the real party in interest in FCA actions, it is not a "party" to a *qui tam* action unless it decides to intervene. The Court said that "to hold otherwise would render the intervention provisions of the FCA superfluous, as there would be no reason for the United States to intervene in an action in which it is already a party."

The Court also said that the United States' status as a "real party of interest" in a *qui tam* action does not "automatically convert it into a 'party'." Rather, the Court said, the phrase *real party in interest* is a "term of art utilized in federal law to refer to an actor with a substantive right whose interests may be represented in litigation by another." The Court further noted that Congress' choice of the term party in Rule 4(a)(1)(B), instead of the phrase real party in interest, demonstrates Congress' intent that the 60-day time limit only apply when the United States is an actual *party* in *qui tam* actions.

The Court also rejected the petitioner's argument that the underlying purpose of the 60-day limit would be best served by applying it in every FCA case. The petitioner argued that even in cases in which the government did not intervene at the district court level, it may want to do so for purposes of the appeal and should have the full 60 days to decide. However, the Court found that "regardless of the purpose of Rule 4(a)(1)(B) and the convenience that additional time may provide to the Government, this Court cannot ignore the Rule's text, which hinges the applicability of the 60-day period on the requirement that the United States be a 'party' to the action."

As such, the Court affirmed the Second Circuit's decision.

> statement that an obligation under the FCA includes "the retention of an overpayment." . . . The Committee also recognizes that there are various statutory and regulatory schemes in Federal contracting that allow for the reconciliation of cost reports that may permit an unknowing, unintentional retention of an overpayment. The Committee does not intend this language to create liability for a simple retention of an overpayment that is permitted by a statutory or regulatory process for reconciliation, provided the receipt of the overpayment is not based upon any willful act of a recipient to increase the payments from the Government when the recipient is not entitled to such Government money or property. Moreover, any action or scheme created to intentionally defraud the Government by receiving overpayments, even if within the statutory or regulatory window for reconciliation, is not intended to be protected by this provision.

S. Rep. No. 111-10, at 15 (2009), *available at* 2009 U.S.C.C.A.N. 430, 442.

The legislative history does not draw a bright line between a permissible and impermissible time period for retaining an overpayment, but it appears that Congress intended that the temporary retention of an overpayment could lead to FCA liability if the overpayment is retained beyond the prescribed reconciliation period or if, prior to the close of a reconciliation period, an overpayment is obtained willfully.

The text of the statute creates liability when an overpayment is retained "knowingly and improperly," which includes situations in which a provider may not have actual knowledge of an overpayment, but nonetheless should have known that it received an overpayment. Thus, the amended FCA creates a potential ticking time bomb for health care providers that receive an overpayment of federal funds.

There are numerous opportunities for a provider to receive an overpayment from a federally funded health care program without necessarily having actual knowledge of the overpayment. For example, the OIG's Work Plan for fiscal year 2010 highlights examples of potential overpayments currently being scrutinized that may lead to liability under the amended FCA:

- Recovery of overpayments from hospitals due to duplicate GME payments;
- Recovery of overpayments from skilled nursing facilities due to use of incorrect RUG scores;
- Recovery of overpayments from physicians due to incorrect payment of e-prescribing incentives;
- Recovery of overpayments from clinical laboratories due to incorrect unbundling of panel tests;
- Recovery of overpayments from DME suppliers due to incorrect documentation to support medical necessity for power wheelchairs;
- Recovery of overpayments from Medicare Advantage plans due to incorrect status designations of enrollees as institutionalized, Medicaid eligible, or ESRD;
- Recovery of overpayments from Part D sponsors due to incorrect prescription drug event data.

provider's receipt of funds from a federal health care program — that a provider knows, or should know, amounts to an overpayment — now involves an enhanced risk of liability. Thus, it is more critical than ever for providers to have systems in place that will detect — and refund — any overpayment of federal funds.

Liability for False Records

The prior version of the FCA made it unlawful to make or use a false record to "get" a claim paid by the federal government. The Supreme Court in *Allison Engine Co. v. U.S. ex rel. Sanders*, 128 S. Ct. 2123 (2008), concluded that such language in the statute created liability only when a defendant made a false record or statement with the intent that the claim for payment would be paid by the federal government (rather than another entity). Congress soundly rejected the Supreme Court's interpretation of the statute by deleting the FCA provision relied upon by the Supreme Court in *Allison Engine* and adding a provision that creates liability for an entity that "knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent *claim*." 123 Stat. at 1621 (to be codified at 31 U.S.C. § 3729(a)(1)(B)).

The defined terms in that statutory provision reveal the expanded scope of the amended FCA. A claim means "any request or demand, whether under a contract or otherwise, for money or property and whether or not the United States has title to the money or property, that (i) is presented to an officer, employee, or agent of the United States; or (ii) is made to a contractor, grantee, or other recipient, if the money or property is to be spent or used on the Government's behalf or to advance a Government program or interest, and if the United States Government (I) provides or has provided any portion of the money or property requested or demanded; or (II) will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded. . . ." 123 Stat. at 1622-23 (to be codified at 31 U.S.C. § 3729(b)(2)). A false record is considered to be *material* if it has a "natural tendency to influence, or [is] capable of influencing, the payment or receipt of money or property." 123 Stat. at 1623 (to be codified at 31 U.S.C. § 3729(b)(4)). Furthermore, a record is *knowingly* false if the defendant had actual knowledge of the falsity or acted with "deliberate ignorance" or "reckless disregard" as to the truth or falsity of the record.

Liability under the "false record" provision of the amended FCA is not limited to payment claims intended to be paid directly by the federal government. Many providers participate in health care programs that are at least partially funded by the federal government. During the course of participating in such programs, providers regularly make and use records in connection with payment claims paid by a variety of entities other than the federal government.

Furthermore, a provider may be liable even if it lacks actual knowledge that a record is false. The statute creates liability if a provider makes or uses a record with "deliberate ignorance" or "reckless disregard" as to the truth or falsity of the record, and the record is "material" to a false claim, i.e., the record would have a tendency to influence payment by the federal government or by another entity acting on behalf of the federal government or advancing a program funded in whole or in part by the federal government.

The false record provision of the amended FCA was given a retroactive effective date of June 7, 2008, and was made applicable to payment claims pending on or after that date. 123 Stat. at 1625. The retroactive effective date was designed to precede the date of the Supreme Court's decision in *Allison Engine*. However, the validity of that retroactive effective date has been called into question. The federal district court to which the *Allison Engine* case was remanded following the Supreme Court's decision has indicated that the

ex post facto

U.S. ex rel. Sanders v. Allison Engine Co., Inc., slip op., No. 1:95-cv-00970-TMR-TSH (S.D. Ohio Oct. 27, 2009). Providers that are currently involved in FCA litigation should consult with legal counsel to evaluate whether they are subject to the prior or the amended version of the FCA.

Accordingly, providers need to implement systems to ensure the accuracy of records that are created or used in connection with payment requests for any health care program that receives funding in whole or in part from the federal government. Obviously, such systems should be tailored to the specific circumstances and needs of each provider, and developed in consultation with a provider's legal counsel.

Liability for Retaliatory Conduct

The prior version of the FCA made it unlawful to retaliate against an employee who attempted to investigate or prevent a possible violation of the statute. The amended FCA extends that protection to contractors and agents, which creates new exposure for health care providers who often deliver services through contractors. See 31 U.S.C. § 3730(h)(1). Any adverse action taken by a provider against a contractor, including, for example, the withholding of payment to a contractor or the termination of a contractor's services, could lead to the contractor's assertion of a "retaliation" claim. Of course, liability remains for retaliatory action against a provider's employees.

Retaliatory conduct not only creates potential financial liability to the employee or contractor, but also is often the impetus for a whistleblower to file a *qui tam* complaint, thereby triggering a federal government investigation with financial consequences far beyond any liability for the retaliatory conduct. Therefore, providers should take steps to minimize the risk that employees or contractors will assert FCA retaliation claims. The appropriate risk management strategies will vary depending on the unique circumstances of each provider and, therefore, should be developed in consultation with a provider's legal counsel.

Conclusion

The FERA amendments to the FCA reflect Congress's intent to maintain the expansive scope of the FCA. The FCA already served as a powerful weapon against the health care industry. In its amended form, the FCA will likely be invoked even more frequently by both the government and qui tam relators as a means to seek financial recovery from the health care industry. Consequently, it is more imperative than ever before that providers utilize effective compliance programs to avoid liability under the FCA.