ROBINSON & COLE LLP
ATTORNEYS AT LAW

Attorney Advertising

UPDATE Health Law Pulse

APRIL 2011

In this Issue...

FEDERAL AGENCIES RELEASE GUIDANCE ON ACCOUNTABLE CARE ORGANIZATIONS

On Thursday, March 31, 2011, the Centers for Medicare & Medicaid Services (CMS), the Department of Health and Human Services Office of Inspector General (OIG), the Internal Revenue Service (IRS), the Antitrust Division of the Department of Justice (DOJ) and the Federal Trade Commission (FTC) all released much-awaited guidance addressing Accountable Care Organization (ACO) requirements for participation in the Medicare Shared Savings Program (Shared Savings Program) established under the Patient Protection and Affordable Care Act of 2010 (PPACA).

CMS released a Notice of Proposed Rulemaking implementing provisions of the PPACA that establish the Shared Savings Program for ACOs. Under the proposed rule, provider participants in an ACO who meet certain quality standards and hold costs below set benchmarks will be eligible for Shared Savings Program payments in addition to the traditional fee-for-service Medicare Part A and/or Part B payments they otherwise receive.

CMS and the OIG also released a notice with comment period describing proposed waivers to the application of the federal Anti-Kickback Statute, the Physician Self-Referral Law and the civil monetary penalties law to specific ACO financial arrangements under the Shared Savings Program.

The DOJ and FTC jointly released a Proposed Statement of Antitrust Enforcement Policy Regarding Accountable Care Organizations Participating in the Medicare Shared Savings Program.

The IRS released a notice and solicitation for public comment, setting forth the circumstances

under which the IRS would generally not view a tax-exempt organization's participation in the Shared Savings Program through an ACO as resulting in inurement or impermissible private benefit to the private party ACO participants.

In the coming week, Robinson & Cole LLP will release a special edition of *Health Law Pulse* describing this new guidance. Additionally, we will present a free Webinar to discuss the highlights of the new ACO guidance on two dates: Wednesday, April 27th from 12:00 to 1:30 p.m. and Wednesday, May 4th from 5:30 to 7:00 p.m.

CMS RELEASES GUIDANCE ON SUSPENSION OF MEDICAID PAYMENTS

On March 25, 2011, the Centers for Medicare & Medicaid Services (CMS) released an informational bulletin (Bulletin) and Frequently Asked Questions (FAQs) on the suspension of payments provision under the Patient Protection and Affordable Care Act of 2010 (PPACA). Under PPACA and its implementing regulations, CMS can suspend Medicaid reimbursement payments to a state for claims submitted by a specific provider or supplier when that state fails to suspend payments to the provider or supplier during an investigation based on a credible allegation of fraud. The Bulletin and the FAQs provide helpful guidance to providers and suppliers on the implications of the regulations.

Medicaid agencies have long been authorized to suspend payments for fraud or willful misrepresentation. However, PPACA and its regulations permit CMS to withhold federal financial assistance from state Medicaid agencies who fail to suspend payments to providers during a pending investigation of a credible allegation of fraud. While payments to providers for emergency items or services are not affected by this suspension, payment may be withheld for nonemergency items or services furnished in a hospital emergency room. PPACA and its regulations do not require a provider to receive advance notification of suspension. However, a provider must be notified within five days of the suspension being imposed. Suspensions may continue until either the investigation reveals insufficient evidence or all legal proceedings related to the provider's fraud are completed.

The FAQs address 20 issues regarding various aspects of suspension authority, including the definition of "credible allegation of fraud," potential sources of such allegations, the actions states should take upon receiving an allegation, and the discovery of billing errors unrelated to the allegation of fraud.

The FAQs define a "credible allegation of fraud" as an allegation that has indicia of reliability. The FAQs note that states are granted flexibility to determine what constitutes a credible allegation based on state law, and give examples of credible allegations of fraud, such as a complaint made by an employee of a physician alleging that the physician has engaged or is engaging in fraudulent billing practices. The FAQs identify potential sources for allegations, including fraud hotlines, claims data mining, civil false claims cases, law enforcement investigations and patterns discovered during provider audits.

According to the FAQs, errors discovered during a provider audit are not considered credible allegations of fraud absent evidence that they are more than "mere errors." The FAQs also state that, in general, billing and processing errors are not considered fraud provided they are "inadvertent."

The FAQs clarify that payment suspensions may only be triggered when the state determines that an allegation of fraud is in fact credible and refers the matter to its Medicaid Fraud Control Unit (MCFU). Note that the MCFU may ask the state not to impose a suspension if it does not want the provider to know there is an investigation pending. CMS may also refrain from

suspending payment at the provider's request or upon a finding that suspension is not in the best interest of the Medicaid program.

COMPLAINTS AGAINST OTHER PHYSICIANS NOT PROTECTED BY PRIVILEGE

On March 23, 2011, a federal district court judge in *Merrick v. Littleton Regional Hospital* (D.N.H., No. 1:10-cv-55-SM, Mar. 23, 2011) held that a physician who alleged that his hospital employer violated the Americans with Disabilities Act of 1990 (ADA), which prohibits discrimination on the basis of disability, as well as a comparable New Hampshire state law, could compel the discovery of hospital peer review records pertaining to other physician employees.

The physician, Dr. Richard Merrick, is an emergency department physician who suffers from both attention deficit hyperactivity disorder and Tourette's syndrome. Dr. Merrick claims that Littleton Regional Hospital in New Hampshire (Hospital) treated him more harshly than it treated other physicians who exhibited similar behavior when it took adverse employment action against him in response to complaints and concerns about his conduct, which was consistent with his Tourette's syndrome diagnosis. The adverse employment action included a suspension, an involuntary leave of absence and a reduction in his hours from 24-hour shifts to 12-hour shifts. During discovery, Dr. Merrick sought records from the Hospital regarding complaints made against other emergency department physicians in order to prove his discrimination claims. Specifically, he requested (i) all complaints made against emergency department physicians during the preceding five years, (ii) a description of the circumstances surrounding such complaints, (iii) investigative actions taken by the Hospital regarding those complaints and (iv) a detailed explanation of the consequences to each physician involved (Requested Records). Dr. Merrick filed a motion to compel disclosure after the Hospital refused to produce the Requested Records.

In response to Dr. Merrick's motion to compel, the Hospital asserted that the Requested Records are protected from disclosure. Specifically, the Hospital argued that the Requested Records are privileged under a New Hampshire state law that protects from disclosure certain records of a hospital committee that is organized to evaluate matters pertaining to the care and treatment of patients, referred to as a quality assurance committee, and testimony by committee attendees relating to activities of the quality assurance committee (Quality Assurance Privilege). Under that law, the Quality Assurance Privilege extends to any information regarding individual physicians provided to a quality assurance committee by a hospital's medical (peer) review subcommittee. The Hospital claimed that its complaint management process is a quality assurance activity and, as a result, records related to complaints against physicians are confidential and protected from disclosure.

The March 23, 2011, order granted Dr. Merrick's request in part. In that order, the judge held that initial complaints made against physicians are not part of a quality assurance process, and therefore, the Hospital was required to provide Dr. Merrick with a list of all complaints made against emergency department physicians in the preceding five years as well as copies of each of those initial complaints, with any identifying information redacted on both the list and the complaints. In addition, the order states that the Hospital must disclose any employment actions, including sanctions placed on physicians, that it took in response to initial complaints in which the complained-of behavior was substantially similar to the behavior exhibited by Dr. Merrick. The judge held, however, that any Hospital records regarding investigations into such complaints are protected under the Quality Assurance Privilege and are not subject to disclosure. In response to the order, Dr. Merrick filed a motion for partial reconsideration.

On March 25, 2011, the judge denied Dr. Merrick's motion for partial reconsideration. In his

motion, Dr. Merrick argued that the order gives too much discretion to the Hospital to identify which complaints involved substantially similar behavior to that of Dr. Merrick. The judge stated that she presumed that the Hospital would make the determination reasonably and would err on the side of broad disclosure. Moreover, the judge noted that if Dr. Merrick believes that the Hospital's production of documents does not comply with the order, he may file an order to compel the Hospital's compliance. In addition, the judge stated that Dr. Merrick is not entitled to statements made in the course of the Hospital's investigation of such complaints because such statements are protected by the Quality Assurance Privilege.

The *Merrick v. Littleton Regional Hospital* case follows a trend of cases which have been limiting the scope of the peer review privilege. While the court protected the Hospital's investigative records and certain peer review proceedings initiated as a result of such initial complaints, it compelled a list of all complaints made against emergency department physicians as well as copies of each of those initial complaints with redacted identifying information. This case confirms that initial complaints will not be considered records protected by the Quality Assurance Privilege in New Hampshire because they arise before the quality assurance or peer review process has begun. Given that the New Hampshire Quality Assurance Privilege is very similar to the peer review statutes of most states, this decision could be followed by other courts construing the peer review statutes of other states. This could have a chilling effect on the submission of complaints regarding the performance of individual professionals and could encourage plaintiffs in employment discrimination cases to seek quality assurance and peer review information of other physicians on the medical staff to support their claims of disparate treatment in violation of law.

PRESCRIPTION INFORMATION INVOLVED IN EPSILON SECURITY BREACH

On April 1, 2011, e-mail marketing company Epsilon Data Management LLC (Epsilon) notified its clients of a security breach involving first and last names and e-mail addresses (Accessed Information) of potentially millions of its clients' customers (Breach).

Many experts believe that the Breach will enable individuals in possession of the Accessed Information to target individual consumers with personalized spam messages, which appear to be legitimate, in order to gain access to additional personal or financial information. Epsilon's 250 clients include major banks, hotels and large retailers, such as Bank of America, Target and Walgreens. At least two large pharmaceutical manufacturers, Astra Zeneca Inc. and GlaxoSmithKline Consumer Healthcare (GSK), were also subject to the Breach.

Epsilon has maintained that Accessed Information did not include more sensitive information, such as personal health, social security or credit card numbers. However, GSK has stated that the files from which the Accessed Information was taken may also identify the GSK product Web site on which customers were registered. Thus, the hackers in possession of the Accessed Information may be aware of the prescription medication taken by certain GSK customers.

On April 16, 2011, GSK sent an e-mail notification (Notification) to customers who had registered on GSK product Web sites informing them that their personal information had been accessed as a result of the Breach. In the Notification, GSK warned its customers about target e-mail messages intended to gain additional information. GSK stated that it would never ask its customers to provide or confirm personal information in e-mails and encouraged customers to delete any e-mail they receive that purports to be from GSK and requests personal information. Even more curious are the isolated reports of people who received GSK's Notification but had never registered at a GSK product Web site.

The Breach highlights the risk of using outside e-mail marketers to manage Web sites as well as the potential risk to health care providers involving similar security breaches of sensitive health information. The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) requires certain entities to notify individuals in the event of a breach of protected health information that is not rendered unusable, unreadable or indecipherable. In addition, depending upon the scope of such breach and the geographic location of the affected individuals, an entity may be required to provide notification to the Department of Health and Human Services, to one or more state attorney general(s), and to the media. You can read more about the HITECH Act's notification requirements here.

It is worth noting that the United States Secret Service is reportedly investigating the Breach. The Secret Service has investigated many large-scale breaches involving financial information as part of its mission to safeguard the nation's financial infrastructure and payment systems. The reason for the Secret Service's involvement in the Breach has not been publicized, but it could suggest at least a concern that personal financial information might be at risk or simply a reliance on the deep experience of the Secret Service in this area, given such a large-scale breach.

If you have any questions about these issues or the content in these articles please contact a member of Robinson & Cole's Health Law Group.

Lisa M. Boyle	Theodore J. Tucci	Stephen W. Aronson
Michael J. Kolosky	Kimberly E. Troland	Pamela H. Del Negro
B. Moses Vargas	Susan E. Roberts	Meaghan Mary Cooper