

Federal Appeals Court Decides When HCQIA Investigations End

Earlier this year, the U.S. Court of Appeals for the First Circuit held that, for the purposes of the physician reporting provisions of the Health Care Quality Improvement Act (HCQIA), an “investigation” remains ongoing until the hospital has concluded its decision-making process. The decision in *Doe v. Levitt*, 552 F.3d 75 (1st Cir. Jan 14, 2009), affirmed the decision of the district court and marked the first time a federal appeals court addressed what constitutes an investigation under HCQIA.

Background

HCQIA requires hospitals to report to the National Practitioners Data Bank (NPDB) any professional review action that adversely affects a physician’s clinical privileges for a period of more than 30 days. The hospital also must report the acceptance of a physician’s surrender of clinical privileges while under investigation for possible professional incompetence or improper professional conduct.

Case Review

In *Doe*, the physician was accused of threatening an emergency room nurse. The hospital temporarily suspended the physician’s privileges and appointed an *ad hoc* committee to investigate the allegations. The *ad hoc* committee reported to the medical staff’s executive committee that the nurse could have reasonably perceived

Hospitals should consider defining what constitutes an “investigation” in the medical staff bylaws and incorporating the Guidebook’s interpretation into their medical staff decisions.

the physician’s actions to be threatening. The executive committee met with the physician and proposed that he be allowed to return to work, provided that he undergo psychological evaluations and monitoring. The physician refused the proposal and resigned. The hospital subsequently reported to the NPDB that the physician resigned while under investigation.

The physician challenged the data bank notification in an administrative appeal, asserting that he resigned after the “investigation” concluded upon the *ad hoc* committee’s report to the executive committee. The administrative judge and district court disagreed, relying instead on the statement by the Secretary of Health and Human Services in the National Practitioner Guidebook, a resource for NPDB users. Per the Guidebook, hospital investigations are “considered ongoing until the health care entity’s decision making authority takes a final action or formally closes the investigation.” The *ad hoc* committee’s report did not signal the conclusion of the investigation, and the physician’s untimely resignation warranted the hospital’s NPDB report.

Practice Points for Hospitals and Physicians

In affirming the decision of the lower court, the First Circuit seems to have created a rigid framework in which the hospital and physician should take caution in discussing potential resolutions to an ongoing investigation. Hospital review committees should therefore

in this issue

- 1 Federal Appeals Court Decides When HCQIA Investigations End
- 2 OIG Announces Plans to Prevent Fraud and Abuse of ARRA Funds
- 3 Update: Amendment to New Jersey’s Codey Act Signed
- 4 The Breach Notification Provisions of the HITECH Act

be certain to communicate to the target of an investigation the context and timeline of the probe. Hospitals should consider defining what constitutes an “investigation” in the medical staff bylaws and incorporating the Guidebook’s interpretation into their medical staff decisions.

Conversely, physicians should be certain that a disciplinary review has reached its completion before contemplating taking action. Any physician under investigation should

be certain that the investigation has run its course before contemplating resignation.

Author:

Andrew J. Siegel

215.981.4043

siegela@pepperlaw.com

OIG Announces Plans to Prevent Fraud and Abuse of ARRA Funds

The Department of Health and Human Services (HHS) is responsible for the disbursement of approximately \$137 billion dollars in federal funds as authorized by the American Recovery and Reinvestment Act of 2009 (ARRA, or the Recovery Act). The funds will be distributed to a broad array of entities in order to expand health care coverage, the health care workforce, and social services related to health care; provide resources for the development of information technology systems in health care; conduct prevention and comparative effectiveness research; and advance biomedical research.

While these funds will provide many opportunities for growth and development within the health care sector, they also provide an important compliance reminder to any entity that will receive a share of ARRA funds, and more generally, to any entity that receives government payments for health care services. Individuals and entities look for value when they spend money during tough economic times, and the government is no exception. As HHS moves to spend the \$137 billion dollars under its control, it will be asking whether or not it is getting good value for its expenditures. An important area of scrutiny will be fraud and abuse.

To this end, the Office of the Inspector General (OIG) announced on April 2, 2009 that it will be doing its part to prevent fraud and abuse of the \$137 billion that HHS will spend under ARRA. The announcement came with an addition to the OIG’s Web site that will publicize the OIG’s efforts in this area. *See* www.oig.hhs.gov/recovery. The Web site describes the OIG’s objectives in this area to include determining whether:

Health care providers who receive ARRA funds should review their policies and procedures to ensure that any funds are used appropriately, and that such use is properly documented.

- funds are awarded and distributed in a prompt, fair and reasonable manner
- the recipients and uses of all funds are transparent to the public, and the public benefits of these funds are reported clearly, accurately and in a timely manner
- funds are used for authorized purposes, and instances of fraud, waste, error and abuse are mitigated
- projects funded under ARRA avoid unnecessary delays and cost overruns, and
- program goals are achieved, including specific program outcomes and improved results on broader economic indicators.

In support of these objectives, the OIG announced several Recovery Act Audit Activities, among them, “launching a Recovery Act risk assessment and work plan development team.” The team is charged with developing an understanding of how each HHS agency (for example the Centers for Medicare and Medicaid Services, or the Agency for Healthcare Research and Quality) plans to

use, disburse and monitor Recovery Act funds. It is likely that in addition to the general task of understanding how HHS will administer Recovery Act funds, the risk assessment and work plan development team will identify various disbursements that are especially at risk for fraud and abuse, and develop methods to audit the use of those funds. Accordingly, health care providers who receive ARRA funds should review their policies and procedures to ensure that any funds are used appropriately, and that such use is properly documented.

More generally, this new initiative by the OIG is an important reminder to all providers, whether they will receive funds under the ARRA or not, to make sure to observe the basics of compliance relative to doing business with HHS: (i) ensure full compliance with Medicare/Medicaid conditions of participation, (ii) monitor physician relationships, (iii) establish sufficient billing and coding procedures, (iv) retain required records in good order, and (v) practice appropriate transparency. In difficult economic times, the government has an additional incentive to watch closely to ensure that it is getting good value for every dollar spent.

Author:

Kevin J. Dill
215.981.4289
dillk@pepperlaw.com

Update: Amendment to New Jersey's Codey Act Signed

Our January 2008 *Health Care Law Update* detailed the threat to ambulatory surgery centers (ASC) in New Jersey posed by the New Jersey Superior Court's 2007 decision to adopt a strict interpretation of the state's laws prohibiting self-referrals by physicians. The court held in *Joseph Garcia, M.D., et al v. Health Net of New Jersey, Inc. v. Wayne Surgical Center, LLC* that referrals of a patient to an ASC in which the referring physician owns an interest violate N.J.S.A. 45:9-22.5, commonly known as the Codey Act. (See http://www.pepperlaw.com/publications_update.aspx?ArticleKey=1048.)

On March 23, 2009, New Jersey Gov. Jon Corzine signed Senate Bill 787, which amended the Codey Act to permit certain referrals to ASCs in which the referring physician has a significant beneficial interest, provided the following four conditions are satisfied:

- the referring physician personally performs the procedure
- the referring physician's remuneration is directly proportional to his or her ownership interest in the ASC, and not to the volume of referrals
- all clinically-related decisions at the ASC are made by practitioners in the best interest of the patient
- the referring physician's beneficial interest in the ASC is disclosed to the patient in writing at or before the time the referral is made.

Additionally, S-787 implements a moratorium on the development of new ASCs in the state, subject to limited exceptions; requires an ASC to (i) register annually with the Department of Health and Senior Services and (ii) obtain accreditation from an accrediting body recognized by Centers for Medicare and Medicaid Services (CMS) within one year of the effective date of the bill.

Author:

Andrew J. Siegel
215.981.4043
siegela@pepperlaw.com

RSS on www.pepperlaw.com

Subscribe to the latest Pepper articles via RSS feeds. Visit www.pepperlaw.com today and click on the RSS button to subscribe to our latest articles in your news reader.

The Breach Notification Provisions of the HITECH Act

Current HIPAA regulations require covered entities to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, the harm caused by security incidents of which the covered entity is aware. Covered entities also are required to document security incidents and their outcomes. But the security rules do not require entities to notify affected individuals of the breach, and entities that comply with HIPAA do not have to comply with most state and federal breach notification laws either. As a result, there is no legal obligation for covered entities to provide notification when personal information, including protected health information (PHI), is lost or stolen in a breach.

The HITECH Act changes this situation by providing new provisions for notifying about breaches, which apply to business associates and covered entities that access, maintain, retain, modify, record, store, destroy or otherwise hold, use or disclose unsecured PHI. A breach is defined as an

unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information...

A breach does not include the unintentional acquisition, access or use of PHI by an employee or individual acting under the authority of a covered entity when made in good faith and within the course and scope of employment or other professional relationship and there are no further actions to acquire, access or use the information. It also does not apply to inadvertent disclosures of PHI within the same facility operated by a covered entity or business associate when the disclosure is from one individual to another and both are authorized to access the PHI.

The term “unsecured” essentially means that the information is unencrypted. Under the HITECH Act, unsecured PHI is not secured by a technology standard that renders PHI unusable, unreadable or indecipherable to unauthorized individuals. Encryption guidelines are to be specified by the secretary of the U.S. Department of Health and Human Services (HHS) or otherwise must

To prepare for the new breach notification requirements, covered entities and business associates should begin by reviewing and updating their current security incident procedures.

meet standards developed or endorsed by the American National Standards Institute.

Discovery of a Breach

Breaches will be treated as “discovered” by a covered entity or a business associate as of the day on which the breach is known or the entity or associate reasonably should have known it had occurred. A breach can be discovered by any person, other than the individual committing the breach, that is an employee, officer or other agent of the covered entity or business associate. Unless delayed for law enforcement purposes, notifications are to be prompt and in no case later than 60 calendar days after discovery of the breach.

Breaches Involving a Covered Entity

Following the discovery of a breach, a covered entity that knows or reasonably believes that unsecured PHI has been accessed, acquired or disclosed as a result of a breach shall notify all affected persons. Notice provided by a covered entity shall include:

- a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known
- a description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number or disability code)

- the steps an individual should take to protect themselves from potential harm resulting from the breach
- a brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches, and
- contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, and e-mail address, Web site or postal address.

Notice may be provided in several ways. First, a written notification may be sent by mail or e-mail. If mailing or e-mail addresses are unknown for 10 or more individuals, substitute notice may be provided. This is accomplished by the covered entity's conspicuous posting on the home page of its Web site or by using major print or broadcast media. When the possible imminent misuse of unsecured PHI creates urgency, notice may be provided to individuals by telephone or other appropriate means. Notice to the media is acceptable when the breach is likely to have included more than 500 individuals.

Breaches involving more than 500 individuals are to be reported immediately to the HHS secretary and will be posted on that agency's Web site. Covered entities will log breaches of fewer than 500 individuals and annually submit the logs to the secretary. The secretary will provide annual notice of all reported breaches to specified House committees.

Breaches Involving a Business Associate

The current security rule provides that a business associate must report to the covered entity any security incident of which it becomes aware. This is very similar to the amended provisions found in the HITECH Act, which provide that following the discovery of a breach, a business associate must notify the covered entity of the breach. The content of the notice is to include the identification of each individual whose unsecured PHI has been (or is reasonably believed by the business associate to have been) accessed, acquired or disclosed during the breach.

Regulations and Effective Date

Interim final regulations on breach notifications are to be published no later than August 16, 2009. The provisions

will become effective and apply to any breach 30 days after publication of the regulations, which is scheduled to be September 15, 2009.

Getting Ready for the New Notification Requirements

To prepare for the new breach notification requirements, covered entities and business associates should begin by reviewing and updating their current security incident procedures. These procedures should name persons responsible for dealing with incidents involving breaches and clearly describe every person's responsibilities during a breach, including:

- methods for providing internal notification of a suspected breach
- steps for taking compromised servers and computers off-line while preserving evidence
- breach investigations, including forensic investigations of computers to determine that a breach occurred, identifying potential causes of the breach and obtaining the names and contact information of people potentially affected
- internal assessment of the breach and determining steps to better prevent future incidents
- analysis of relevant laws to determine the appropriate response and potential liability created by the breach including potential litigation, agency investigations and actions by applicable attorneys general
- preparation of notice response, including determination of the appropriate method of notice (i.e., written or substitute notice) and the notice content for private notification (for individuals), public notification (to the HHS secretary) and, when applicable, notification by a business associate to the covered entity
- steps for the delivery of the notifications of the breach
- methods to respond to inquiries pertaining to the breach and other public relations needs, and
- procedures for responding to litigation or agency investigations.

Author:

*M. Peter Adler
202.220.1278
adlerp@pepperlaw.com*

Don't Miss Future Issues

Be sure to receive future issues of *Health Care Law Update*. Please subscribe online at www.pepperlaw.com, or you may fill out the form below and mail it to Pepper Hamilton LLP, Attn: Kathy Rebecchi, 3000 Two Logan Square, Eighteenth and Arch Streets, Philadelphia, PA 19103-2799, or fax it to Kathy Rebecchi at 215.981.4750.

How would you like to receive this newsletter: E-mail* Mail

Name _____

Title _____

Company _____

Address _____

Phone _____ Fax _____

E-mail* _____

Pepper Hamilton LLP

Attorneys at Law

The material in this publication is based on laws, court decisions, administrative rulings and congressional materials, and should not be construed as legal advice or legal opinions on specific facts. The information in this publication is not intended to create, and the transmission and receipt of it does not constitute, a lawyer-client relationship.

Please send address corrections to phinfo@pepperlaw.com.

www.pepperlaw.com

Berwyn | Boston | Detroit | Harrisburg | New York | Orange County | Philadelphia | Pittsburgh | Princeton | Washington, D.C. | Wilmington

© 2009 Pepper Hamilton LLP. All Rights Reserved.
This publication may contain attorney advertising.