HOOPER LUNDY & BOOKMAN, INC.

HEALTH LAW PERSPECTIVES

Newsletter
Volume 5, No. 3

April 2003

Local Governments Face False Claims Act Liability

On March 10, 2003, the U.S. Supreme Court unanimously ruled that local governments may be liable for charges brought under the federal False Claims Act (FCA). This means that cities, counties and other municipalities (including probably healthcare districts) may be subject to pay treble damages and penalties as a result of FCA actions brought against them.

The Supreme Court had ruled in a previous case that states are not "persons" subject to the *qui tam* (whistleblower) actions under the FCA *(Vermont Agency of Natural Resources v. United States ex rel Stevens* 529 U.S. 765 (2000)). In this case, however, the Court ruled that local governments are subject to such suits and remanded the case for further hearing.

The case involved a National Institute of Drug Abuse research grant to Cook County Hospital for a study that was later administered by a non-profit research institute affiliated with the hospital. The administrator of the study for the institute filed a *qui tam* action, claiming that Cook County and the institute had submitted false statements to obtain grant funds in violation of the FCA.

The fraud in this case allegedly occurred in administering a $5 million grant from the National Institute of Drug Abuse to Cook County hospital, to study a treatment regimen for pregnant drug addicts. The grant was subject to a variety of conditions, including terms of a compliance plan devised to ensure that the study would comply with federal regulations for research on human subjects. Administration of the study was transferred to the Hektoen Institute for Medical Research, a non-profit research organization affiliated with the hospital. The respondent ran the study from September 1993 until the institute fired her in January 1995.

In 1997 the respondent filed a *qui tam* action claiming that the county and institute had violated the grant's conditions, had failed to comply with the regulations on human-subject research and had submitted false reports of what she called "ghost" research subjects. The respondent also alleged that she was fired for reporting the fraud to doctors at the hospital and to the granting agency, rendering her dismissal a violation of both state law and whistleblower provision of the FCA.

The government initially declined to intervene in the action and the county moved to dismiss the claims against it, arguing that it was not a "person" subject to liability under FCA. The district court denied the motion, reading the term "person" in the FCA to include state and local governments. The court of appeals dismissed the county's appeal and the U.S. Supreme Court denied a request to hear the case.

After the *Stevens* decision, however, the district court reconsidered the

In this issue:

Hooper Lundy & Bookman, Inc.

HEALTH CARE LAWYERS

county's motion and dismissed the whistleblower's action. Although the court found "no reason to alter its conclusion that the county is 'person' for purposes of FCA," it held that the county, like a state, could not be subjected to treble damages, which it described not as "remedial" but as "essentially punitive." The court of appeals, in conflict with two other circuits, reversed the lower court decision. The U.S. Supreme Court then granted review and affirmed the appellate court decision.

Under the FCA, "[a]ny person" who "knowingly presents, or causes to be presented, to an officer or employee of the United States Government. . . a false or fraudulent claim for payment or approval" is liable to the government for a civil penalty, treble damages, and costs.

At issue was whether a local government may be considered a "person" for purposes of the FCA. In its ruling, the Court noted that since its passage in 1863 there has been no doubt that the act applies to corporations and found that "neither the history nor the text of the original FCA provides contextual evidence that Congress intended to exclude municipalities from the class of "persons" covered by the FCA.

Further, the court found that the False Claims Amendments Act of 1986 did not repeal municipal liability. As part of the a 1986 amendments, the ceiling on recoverable damages was raised from double to treble. The Court rejected the county's argument that since the damages amount escalated from "remedial" to "punitive" , municipalities were automatically excluded from FCA liability because punitive damages may not generally be levied against municipalities.

"Inferring repeal of municipal liability from the increase in the damages ceiling from double to triple would be difficult in the abstract, but it is impossible given that the basic propose of the 1986 amendments was to make the FCA a more useful tool against fraud in modern times," the court said.

The Supreme Court ruling leaves counties, cities and other municipalities liable for treble damages and penalties under the FCA. The reasoning will likely also apply to district health care entities. However, in determining whether to settle a case or proceed to trial, local governments should consider all possible defenses. Such damage awards, for example, may be subject to reduction under the Excessive Fines Clause of the Eighth Amendment of the Constitution . Under that clause, a fine is considered unconstitutionally excessive if it grossly disproportionate to the gravity of the offense.

In a case currently awaiting hearing by the Ninth Circuit Court of Appeals, Hooper Lundy & Bookman is representing a defendant found liable for violating the FCA and levied with treble damages (*U.S. v. Mackby,* No. 99-15605). On behalf of the defendant, HLB is arguing that the damages levied upon this defendant are excessive under Eight Amendment. The case is expected to be heard in May or June of this year.

For more information, please contact Patric Hooper, Lloyd Bookman or John Hellow in Los Angeles at (310) 551-8111 or Mark Reagan in San Francisco at (415) 875-8501.

CMS Proposes Changes to Outlier Payment System

The Centers for Medicare & Medicaid Services (CMS) has proposed new regulations devised to prevent "gaming" of the outlier system.

According to CMS, the outlier spending targets were $3.5 billion in 2000 and actual spending was $5.3 billion; $3.6 billion in 2001 while spending was $5.5 billion; and $3.7 billion for 2002, while spending was $5.3 billion.

The proposed rule builds on actions CMS took in December to identify hospitals that appear to have employed charging strategies designed to maximize outlier payments.

Under current rules, in order to estimate the actual costs incurred by a hospital for a given case, Medicare uses the historical relationship between each hospital's costs and its charges. So long as hospital costs and hospital charges change at roughly the same rate, this estimate produces a relatively reliable result. However, if a hospital increases its charges dramatically relative to costs, the use of the historical relationship will yield higher outlier payments than would be appropriate, according to CMS. In addition, the longer the lag between the historical data and the current charges — currently two years - the less accurate the estimate will be.

Each year, when CMS updates the hospital payment rates, it sets a fixed-loss threshold for outlier payments designed to keep them at the target of 5.1 percent of total DRG payments. As outlier claims increased, the outlier threshold has gone up sharply — from $14,050 in 2000 to $33,560 in 2003 to stay within the 5.1 percent target. As a direct result, more hospitals have had to absorb the costs of complex cases according to CMS.

The rule proposes three significant changes to prevent hospitals

from manipulating the outlier formula:

- It allows Medicare to use more recent data to calculate outlier payments.
- It eliminates the use of a statewide average ratio of costs to charges for hospitals with very low computed cost-to-charge ratios.
- It allows Medicare to recompute outlier payments after a fiscal year by applying cost to charge ratios determined from a hospital's settled cost report and to recover any overpayments, or, presumably, to pay any underpayments.

Overpayment recoveries would be subject to an adjustment to account for the value of the money during the time period it was inappropriately held by the hospital.

For more information, please contact Lloyd Bookman at (310) 551-8185 or lbookman@health-law.com.

CMS Issues Final HIPAA Security Standards,Clarifies EDS Regulations

By Elspeth Delaney

The Centers for Medicare and Medicaid Services (CMS) has issued two sets of final regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). First, CMS finalized the Security Standards (the Security Regulations). Second, CMS clarified certain aspects of the Electronic Data Transaction Standards and Code Set Regulations (EDS Regulations).

Security Regulations

The good news is the final Security Regulations, issued on February 20, 2003, are simpler and give "covered entities" greater flexibility in determining how to meet the requirements. The bad news is that the compliance plans, policies and procedures, and business associate contracts that everyone has been busy implementing under the HIPAA privacy regulations will all need to be revised to address the Security Regulations.

The compliance deadline is April 21, 2005 (except for small health plans, which have an additional year). There may, however, be a technical correction to this deadline in the near future.

The Security Regulations apply to a subset of the information covered under the Privacy Regulations - namely electronic protected health information (e-PHI). e-PHI is defined as individually identifiable health information that is transmitted by or maintained in electronic media. e-PHI does not include paper to paper faxing or voice telephone communications. e-PHI is protected under the Security Regulations whether being transmitted internally within a covered entity or externally, and whether located on systems at the covered entity or at its workforce's other locations (such as their homes).

A covered entity has the following general responsibilities under the Security Regulations:

- Ensure the confidentiality, integrity, and availability of all e-PHI the covered entity creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Regulations; and
- Ensure compliance with the Security Regulations by its workforce.

Unlike the proposed security regulations, the final Security Regulations provide a flexible approach to compliance. The Security Regulations are divided into standards and implementation specifications. Where a standard has no implementation specification, the stan-

Orthopaedic Hospital Case Payment Approved

We are pleased to report that the federal district court in the *Orthopaedic Hospital* case has just signed the order we presented approving the distribution of approximately $132.5 million to California hospitals. We expect the funds to be delivered by the California Healthcare Association within the next week or two. This is in addition to the $28.9 million in payments that have recently been mailed in the *Barlow Community Hospital* case.

We continue to work with the federal government to obtain federal matching funds. We are hopeful that those funds can be secured in the near future.

For additional information, please contact Lloyd Bookman at (310) 551-8185 or lbookman@health-law.com

dard itself is the instruction on how to implement the standard. The implementation specifications are either "required" or "addressable." A "required" implementation specification must be implemented as described. A covered entity must assess an "addressable" implementation specification to determine whether the implementation specification is a reasonable and appropriate safeguard in the specific covered entity's environment and then either:

- Implement the implementation specification if reasonable and appropriate; or
- If implementing the implementation specification is not reasonable and appropriate: (1) document why it would not be reasonable and appropriate to implement the implementation specification; and (2) implement an equivalent alternative measure if reasonable and appropriate.

In deciding which security measures to use, a covered entity must take into account the following factors:

- The size, complexity, and capabilities of the covered entity;
- The covered entity's technical infrastructure, hardware, and software security capabilities;
- The costs of security measures; and
- The probability and criticality (seriousness) of potential risks to e-PHI.

The chart on page 5 shows which standards have implementation specifications, whether the implementation specification is required or addressable, and whether policies and/or procedures are required for the topic. The standards are divided into three categories: Administrative Safeguards (e.g., how a covered entity operates), Physical Safeguards (e.g., how a covered entity protects physical access) and Technical Safeguards (e.g., how a covered entity protects technical/information access). The categories are shown in bold, the standards are shown in italics and the implementation specifications are shown in plain text.

EDS Regulations Update

The EDS Regulations require "covered entities" under HIPAA to use prescribed transaction standards for eight different transactions: (i) Health Care Claims or Equivalent Encounter Information; (ii) Eligibility for a Health Plan; (iii) Referral Certification and Authorization; (iv) Health Care Claim Status; (v) Enrollment and Disenrollment in a Health Plan; (vi) Health Care Payment and Remittance Advice; (vii) Health Plan Premium Payments; and (viii) Coordination of Benefits. There are two other types of transactions for which CMS has not yet issued transaction standards - first report of injury and health claims attachments.

Compliance Issues

CMS recognized that there has been a lot of confusion regarding the compliance dates for the EDS Regulations. Covered entities are required to comply with the EDS Regulations by October 16, 2002, unless they filed an extension or are a "small health plan," in which case the compliance deadline is October 16, 2003. The revised final EDS Regulations do not change these compliance dates but state that a covered entity that was required to comply with the transaction standards by October 16, 2002, does not have to comply with the *revised* transaction standards until October 16, 2003. CMS stated: "We will not invoke our authority to penalize noncompliance with [revised] standards that our own delay in issuing this final rule has made infeasible."

In addition, CMS clarified that a covered entity only needs to comply with the transaction standards when conducting a transaction with another covered entity required to comply with the transaction standards. CMS explained that if both sides to a transaction are not required to conduct the transaction in standard from (that is, if one side is required to conduct the transaction in standard form but the other side is not), neither side is required to conduct the transaction in standard form. For example:

- If a physician who is not a covered entity under HIPAA submits a bill to a health plan that is a covered entity, the bill does not need to meet the requirements of the transaction standards.
- If small health plan is coordinating care with a health plan currently compliant with the transaction standards, the coordination of care transaction does not need to meet the transaction standards requirements until October 16, 2003.
- If a hospital filed an extension and bills a health plan that is currently compliant with the transaction standards, the billing transaction does not need to meet the requirements of the transaction standards until October 16, 2003.

Adoption of Codes

CMS has adopted the National Council for Prescription Drug Programs (NCPDP) standards for the

(continued on page 5)

Standard/Implementation Specifications	*Required (R) or Addressable (A)?*	*Policy and/or Procedure Required?*
Administrative Safeguards		
Security Management		Yes
Risk analysis	R	
Risk management	R	
Sanctions for workforce	R	
Assignment of Security Officer	R	
Workforce Security		
Authorization and Supervision of workforce working with e-PHI or where e-PHI accessible	A	
Workforce clearance procedure	A	
Workforce termination of access procedure	A	
Information Access Management		Yes
Isolate clearinghouse functions of hybrid	R	Yes
Access authorization for workstation and software programs	A	Yes
Access establishment and management (review and modification)	A	Yes
Security Awareness and Training		
Security reminders	A	
Protection from malicious software	A	Yes
Log-in monitoring	A	Yes
Password management	A	Yes
Security Incidents		Yes
Response, reporting and documenting security incidents and outcomes	R	
Contingency Plan		Yes
Data back-up plan	R	Yes
Disaster recovery plan	R	Yes
Emergency mode operations plan	R	Yes
Testing and revision of contingency plan	A	Yes
Application and data criticality analysis	A	
Evaluations and periodic testing of technical and non-technical aspects of security		
Business Associates		
Written business associate contracts with specific security language	R	
Physical Safeguards		
Facility Access		Yes
Contingency operations	A	Yes
Facility security plan	A	Yes
Access control and validation procedures	A	Yes
Maintenance records	A	Yes
Workstation use		Yes
Workstation security		
Device and media controls		Yes
Disposal	R	Yes
Media reuse and recycling	R	Yes
Record of movements of hardware and electronic media	A	
Data backup storage	A	
Technical Safeguards		
Access Control		Yes
Unique user identifiers	R	
Emergency access procedure	R	Yes
Automatic log-off	A	
Encryption and decryption	A	
Audit controls to record and examine activity in information system		
Integrity of data maintained so can corroborate no unauthorized alteration or destruction of data		
Mechanism to authenticate e-PHI	A	
Person or entity authentication		Yes
Transmission security for e-PHI in transit		
Integrity controls	A	
Encryption	A	

Adoption of Codes

(continued from page 4)

following retail pharmacy transactions as the standard for the referral of certification and authorization transaction and has adopted the Accredited Standards Committee (ASC) X12N 835 as the standard for payment and remittance advice. CMS has decided to continue using the National Drug Codes (NDC) as the standard for reporting of drugs and biologics.

If you have any questions regarding the new regulations or HIPAA, please contact Elspeth Delaney at (310) 551-8138 or edelaney@health-law.com.

CALENDAR

April 2-4	HLB Attorneys Lloyd Bookman, John Hellow and Jon Neustadter speak at the American Health Law Association Institute on Medicare and Medicaid payments at the Baltimore Marriott Waterfront. Mr. Bookman will moderate a Provider Reimbursement Review Board panel, Mr. Hellow will speak on recent disproportionate share hospital litigation, Mr. Neustadter will speak on PRRB practice and jurisdiction.
May 24	HLB Attorney Jodi Berlin speaks on *Survey Recovery* at the annual conference of the California Association for Health Services at Home, Sacramento Convention Center.

Hooper Lundy & Bookman, Inc.

HEALTH CARE LAWYERS

1875 Century Park East, Suite 1600
Los Angeles, California 90067-2799

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE
PAID
NASHVILLE, TN
PERMIT 989