CCH Healthcare Compliance LETTER

Volume 6, Issue 18 www.cchgroup.com September 15, 2003

AHA responds to recent CMS guidance

by Sharon Sofinski

In a recent letter to the National Committee on Vital and Health Statistics (NCVHS), the American Hospital Association (AHA) asked NCVHS to urge the Centers for Medicare and Medicaid Services (CMS) to respond quickly to "critical issues" not addressed in CMS's recent guidance on compliance with the HIPAA transaction and code sets standards. See "NCVHS rejects TCS extension; CMS issues guidance," *CCH Healthcare Compliance Letter*, Volume 6, Issue 17.

Uninterrupted payment. AHA's first concern is that although the CMS guidance recognized the importance of uninterrupted payment for providers, it did not create a safety net to ensure that providers will continue to receive payment for services after October 16, 2003, the HIPAA compliance deadline. The AHA expressed the need for a contingency plan that outlines specific steps to reduce the "most harmful consequences of implementation—disruptions to the payment cycle."

Nonmaterial claim errors. The AHA letter also asks that CMS clarify whether a plan will be in violation of HIPAA if it processes a claim that complies with HIPAA format and code sets requirements but contains nonmaterial errors.

The current lack of guidance, AHA believes, means that some health plans will reject an entire batch of claims when only one or a few of the individual claims in the batch contain errors. That would be a costly and inefficient way to process claims, AHA argues. AHA calls on CMS to issue a guidance clarifying that health plans should *not* reject the entire batch of claims in such a situation.

Good-faith efforts. AHA also believes that CMS should outline specific good-faith efforts covered entities should take before the October 16 deadline. With regard to testing the transactions with providers, AHA has learned that many hospitals are frustrated that they are unable to test with many health plans and that some testing schedules begin too late to demonstrate a good-faith effort to comply.

AHA's letter stressed the need for CMS to act quickly on these issues. "CMS' failure to act decisively on these remaining issues will only prolong the confusion and difficulty arising with implementation of the standards and will increase the possibility of large-scale payment disruptions." The full text of the AHA letter is at http://www.hospitalconnect.com/aha/key_issues/hipaa/transactions/NCVHS082103.html. ■

CCH Chicago Bureau, September 2, 2003

Letters to the Editor

The CCH Healthcare Compliance team welcomes comments or questions regarding articles published in the CCH Healthcare Compliance Letter. Send comments to Raio G. Krishnayya, Coordinating Editor, at krishnar@cch.com. For more information about the CCH Healthcare Compliance Portfolio visit our online store at http://health.cch.com.

Excessive Fines Clause challenge unsuccessful: Future challenges difficult to predict

by Raio G. Krishnayya, J.D.

There are many legal doctrines available in the arsenal of the defense attorney that can be used to defend a False Claims Act (FCA) suit. However, this last year has seen the emergence of a unique argument with regard to the damages phase of a case—the Excessive Fines Clause of the Eighth Amendment of the U.S. Constitution. Unique as this argument is, its relatively sparse history makes such a challenge extremely unpredictable and reveals the highly subjective rationale a court can adopt in determining such cases.

The case, *U.S. v. Mackby*, originated in 1998, when Peter Mackby was sued by the U.S. government for unauthorized use of his father's personal identification number (PIN) to obtain Medicare Part B payments. Generally, Part B pays for services not covered under Medicare Part A, such as physical therapy, under two conditions. The first condition is when a physician or qualified employee of a physician provides physical therapy services. Under this condition, there are no payment limitations imposed on the services rendered. The second condition occurs when the physical therapy service is rendered by a qualified physical therapist in an independent practice (PTIP). Medicare Part B does impose payment limitations for services rendered pursuant to physical therapy under a PTIP.

Mackby, neither a physician nor qualified physical therapist, jointly owned a physical therapy clinic with a qualified physical therapist. During the joint ownership, the clinic billed for Medicare Part B payments using the physical therapist's personal identification number (PIN). Several years later, Mackby became sole proprietor of the clinic and used his father's, a physician, PIN to bill for Medicare Part B services. According to the government, Mackby submitted 8,499 false claims for payment.

Procedurally, Mackby went to trial and was found to have violated the FCA. However, instead of seeking damages for all 8,499 claims, the government sought restitution for the amount that exceeded the Medicare annual payment limit per beneficiary for the PTIPs. Coupled with the imposition of treble damages, the court imposed a judgment in the amount of $729,454.92.

Excessive fines. Mackby appealed the finding of liability under the FCA as well as the imposition of the damages. The U.S. Court of Appeals for the Ninth Circuit affirmed the trial court's finding; however, the Ninth Circuit held that the damages clause of the FCA was punitive in nature and possibly subject to an Excessive Fines Clause challenge.

Notably, Mackby applied the Excessive Fines Clause challenge to both the civil penalty and damages components of the trial court's order. The Ninth Circuit, in remanding the case back to the trial court for further findings, addressed this point.

> In remanding this case to the district court to apply an excessive fines analysis to the civil penalty and the treble damages portions of the case, we recognize that the amount of the civil penalty and the amount of treble damages need not be considered in isolation as if the other did not exist. CCH ¶301,425.

Upon remand, the trial court held that the total amount owed by Mackby, $729,454.92, was not excessive in light of the fact that Mackby faced $85 million in civil penalties in addition to $1 million in treble damages. Also, the trial court found that the government suffered "significant harm" in light of Mackby's conduct; hence, it concluded that the amount imposed was not "grossly disproportional to the gravity" of Mackby's offense.

Mackby appealed these findings to the Ninth Circuit. The Ninth Circuit upheld the trial court's findings with regard to Mackby's Excessive Fines challenge. However, the current round of appeals illustrates some of the public policy considerations that weigh at the heart of this unique challenge to the damages clause of the FCA.

No harm, no foul. An Excessive Fines challenge requires the appellant to show the existence of two conditions:

- The damages imposed is a *punishment* in response to particular conduct, and
- The damages are *grossly disproportionate* in comparison to the offense proscribed.

Under the Mackby argument, the offending conduct was that he used his father's PIN number without proper authorization. In other words, the underly-

continued on page 3

Comments from readers are welcome and should be directed to Raio Krishnayya at KRISHNAR@CCH.COM, Tel. 847-267-7316, Fax 847-267-7040. Customer service inquiries should be directed to 800-449-9525.

CCH Healthcare Compliance Letter is published 24 times a year by CCH INCORPORATED, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is $305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO *CCH Healthcare Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

ing claims submitted for payment were not false because Mackby legitimately owned the physical therapy clinic, **and** the claims for services rendered were in fact actually rendered. Thus, under the Mackby assertion, if the offending conduct was not having proper authorization, then the $729,454.92 is grossly disproportionate.

The Ninth Circuit disagreed. Reading into the legislative intent of the framers of the FCA, the Ninth Circuit found that belying the enactment of the FCA was not only an intent to deter claims that should not have been submitted, but also an intent to maintain the integrity and administration of the billing system.

> In the legislative history to the FCA, Congress specifically rejected a "no harm, no foul" argument. Fraudulent claims make the administration of Medicare more difficult, and widespread fraud would undermine public confidence in the system.

Criminal vs. civil. Equally interesting was Mackby's comparison of the monetary penalties under the criminal FCA versus those imposed under the civil FCA. Mackby asserted that under the criminal FCA, the most he could be fined would be $75,000 as compared to almost $730,000. The Ninth Circuit found that the flaw in this argument was that it failed to account for the potential sentence of incarceration that could be imposed pursuant to the federal Sentencing Guidelines. In Mackby's case, had the government secured a conviction under the criminal FCA, Mackby would have faced between 37-46 months of incarceration, in addition to restitution of up to $75,000. Furthermore, the Ninth Circuit noted that courts making such comparisons between criminal and civil penalties almost always consider the incarceration element as significant.

On the other hand, the case that weighed heavily in the Ninth Circuit's analysis was *U.S. v. Bajakajian*, 524 U.S. 321 (1998). That case stands as the rare successful Excessive Fines Clause challenge. *Bajakajian* involved a forfeiture of the defendant's personal funds for failing to accurately declare the amount of money he had in his personal possession to U.S. Customs officials. The Supreme Court noted that the forfeiture was "grossly disproportionate" (the seizure of over $300,000 of the defendant's personal funds) in comparison to the relatively minor reporting offense.

However, *Bajakajian* becomes somewhat ambiguous in the light of *Mackby*, especially with regard to the argument that compares criminal and civil penalties. In *Bajakajian*, the Supreme Court used the potential $5,000 fine and six-month incarceration as a benchmark against the over $300,000. Recall that Mackby asserted a similar argument, comparing the potential punishment under the criminal FCA and his current damages. Yet, the Ninth Circuit cryptically dismissed the argument stating, "The substantially greater criminal penalties that Mackby hypothetically could have faced for his conduct do not 'confirm a minimal level of culpability.'"

Key points. Recall that the standard for an Excessive Fines challenge is whether the damages imposed are "grossly disproportionate" to the conduct being punished. This standard seems highly subjective. Relatively sparse, the history of Excessive Fines Clause challenges leaves little more than a laundry list of what are and what are not considered "grossly disproportionate" fines.

For example, the Ninth Circuit's own reading into how it has reviewed Excessive Fines Clause challenges leaves these factors:

- Considerations of whether other illegal activity was involved;
- Whether the illegal profit was larger than the fine;
- Whether defendant could have elected for alternate punishment instead of monetary penalty; and
- Pursuant to *Mackby*, whether the defendant's conduct also impaired the administration of a federally reimbursable program.

Thus, at best, *Mackby* adds another tile to the confusing picture of when an Excessive Fines Clause challenge might be successful. At worst, this case illustrates the highly subjective nature of this protection with little to objectively guide the hands that are charged with making such decisions. ■

United States v. Mackby, 9th Cir., No. 02-16778, Aug. 12, 2003, ¶301,470

Creating an effective HIPAA security plan

by Catherine Hubbard, MA

Many health care facility operators are still puzzling over how to set up security systems that comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. It can be done, however, with proper planning and effective use of resources, according to experts who were recently interviewed.

Security safeguards are crucial, since they set the framework for all of HIPAA compliance, said Richard Marks, a partner at the Washington D.C. office of Davis Wright Tremaine. "Security is fundamental to privacy."

Getting started

With an April 21, 2005 compliance date for most companies, those that have not already begun a compliance program should start now, said Gretchen Hellman, senior products manager at Network Associates Expert Services, Santa Clara, California. "The time to get started was 6 months to a year ago."

It's also the right time to start planning for the costs of compliance programs and training, said Cynthia E. Smith, Senior Manager of Technology and Data Services at PricewaterhouseCoopers, Pittsburgh, noting that most companies are putting together their budgets for fiscal years 2004 and 2005. "If they are going to put money into compliance that should be in the budget cycle now."

Covered entities should immediately do several things that are relatively inexpensive such as conducting employee training programs, developing sensible business processes that incorporate security protections and making simple changes in the configuration of existing equipment so the systems are harder to hack, Marks said. "All of these can be done quickly and effectively."

In addition, any hospital, health plan, or clearinghouse that wants to buy electronic data processing systems should negotiate security features from the very beginning, said Marks. Computer systems software and telecommunications systems have a development cycle, he said. "Security has to be a part of that life cycle from the start."

Don't waste time

Administrators should get a clear understanding of the problem before taking any action in order to avoid spending time and money on duplicative processes, said Hellman. Marks noted that businesses should make strategic choices early on with regard to HIPAA security. "Many of these decisions are based on legal, budgetary and operational considerations," Marks said. "They all have to be mixed in carefully. "

The right technology products might also help save time and money, but should not be the main compliance tool, Hellman cautioned. "No product will make you HIPAA compliant."

Achieving "buy-in"

The next step is to get employees on board. "Implementing security measures requires a huge cultural change," Hellman said. It is essential to train staff on the new security measures, she said, noting that a lot of organizations are struggling to get buy-in because of lack of education."Training is critical, particularly when trying to get buy-in."

Managers also must assign each person involved with responsibility for a part of carrying out the security procedures both on a company-wide level and an individual level. "Otherwise, it won't get done," said Hellman. She further noted that HIPAA fines and penalties can fall on individuals. "They need to play their part."

Create a useful manual

Along with training, employers will need to develop intelligent policies that are clear and succinct. Writing a 200 to 300-page security policy will not help staff to understand and follow the new measures, said Hellman."Information policies are always too long." Instead, companies should consider breaking them up into shorter pieces. She suggested breaking up the manual into sections that apply to different specialties or to specific end users, such as doctors, nurses and administrators.

Avoiding legal pitfalls

Although a good compliance plan requires risk analysis, managers need to ensure the analysis does not make the company vulnerable to unnecessary legal exposure. "You need to preserve legal privilege right from the start," Marks advised. When a hospital or health plan performs the analysis, they generate a list of vulnerabilities that can be fodder to a trial lawyer, he said. "That list can become Exhibit One for the plaintiffs." Managers should create a sound approach for preserving legal privilege, he said. Although it is never clear that the protection is airtight, he said: "It is better to have the foundation for arguing legal privilege to the courts."

Restrict access to medical records

As part of ongoing assessment, it's important to keep an eye on who is viewing personal health information (PHI), said Smith. An early version of the Privacy rules would have asked health care organizations to track anytime an individual adds, changes or deletes a medical record. Even though the requirement didn't make it into the final HIPAA Security rules, the fact that it was considered is a warning to operators that they should keep an eye on who has access to computerized records and whether those people are viewing or altering the records, she said.

The final security regulations state that covered entities should review any information security activity for attacks, said Smith. "Each covered entity has to come to grips with what the regulations mean to them."

Entities need to look for unusual patterns of access. For instance, they should track who has logged onto and logged off of the system and the times of day the activity occurred. An entry at 2:00 AM may be appropriate for a 24-hour hospital, Smith said. But if the log-in record indicates that a nurse who works 9 to 5 was accessing the system in the middle of the night, it may be suspect.

Another factor to watch is whether the person accessing the system is authorized and whether he or she would have a good reason to view the records. A nurse who does not work in the maternity ward should not be accessing the records of a friend who just had a baby, Smith said. A caregiver who has performance issues also should be watched closely, she said, noting that it should not be a legal problem if human resources needs to examine his or her online activity.

Smith stressed that each entity should determine what activity it will find acceptable and set up business processes to support those determinations. It should talk to all employees about what they will and will not be allowed to do. "HIPAA is not an IT problem. It's a business processes issue. "

PHI in e-mails

Operators also need to think through how they want to handle e-mail in light of the Security rules. Many doctors and patients have found e-mail a useful tool to help with the diagnosis and treatment of conditions. However, the information could be intercepted by hackers.

Smith advised entities to decide whether to encrypt e-mails, how much encryption to use, whether doctors and hospitals should be permitted to send e-mails to each other or whether doctors may only send e-mails to patients and whether e-mails should be permitted to contain personal health information. The Centers for Medicare & Medicaid Services has said that the decision to encrypt is an addressable item, meaning that companies should decide what is best for them.

There are various ways to handle the security challenges e-mail presents. Some companies may believe an e-mail with PHI is "a needle in a haystack" and does not pose a serious security risk, Smith said. Others might be more cautious and instruct doctors to notify patients that e-mail is an insecure method of communication or to ban such e-mails altogether.

Document everything

Making good decisions and having good security systems in place is not enough to comply with the HIPAA Security regulations. Any security measures the company does implement, need to be documented. The rules also require a well-documented security management process, said Marks. "Documentation of business decisions and the basis for those decisions, particularly for the so-called addressable implementation specifications in the rules, is a fundamental element of this whole process."

"Document everything, every decision you make, all of the money you are spending on it [and] the hours you spend," Hellman advised.

Be reasonable

Few patients would be comforted by an office that completely restricts access to patients' records. The goal of a good security plan is not to shut down the flow of information that is crucial to good health care, but is to prevent the information from getting into the wrong hands.

Rather than trying to eliminate all risk of security breaches, the company should follow best practices, use due diligence, train staff and decide what level of risk is acceptable, said Hellman. "The problem with security is that nothing is really secure. You can't make [PHI] available and secure." Since it's impossible to completely secure protected health information, operators should focus on due diligence and take a hard look at all of their security measures, she said.

Hellman recommended that health care operators imagine themselves faced with a lawsuit, and think about what security measures they will wish they had taken. From that viewpoint, operators can more clearly assess risk and determine their vulnerabilities. That might free up some of their limited funds on the most important safeguards, she said.

Ms. Hubbard is a reporter in the Washington, D.C. office of CCH INCORPORATED. She has reported on several areas of federal and state policy, including tax, banking, health care, food and drug law, assisted living, long-term care, and laws affecting small businesses. Ms. Hubbard may be contacted via the following: mail---CCH INCORPORATED, a Wolters Kluwer company, 1015 15th St., N.W., 10th Fl., Washington, D.C. 20005; phone---(202) 842-7371; e-mail---hubbardc@cch.com.

Hospitals win increased funding

by Geraldine S. Stroka, J.D., R.N., M.S.N.

Hospitals have won an important victory in the reimbursement battle involving healthcare rendered to undocumented aliens. The Arizona Supreme Court overturned the state's cost containment agency's decisions that denied statutorily-required payments for the care of uninsured patients and established a test for use in determining whether an emergency medical condition exists.

Emergency care funding. The Arizona Supreme Court consolidated three cases and applied Arizona medical care reimbursement statutes in interpreting §1903(v) of the Social Security Act; the statute that defines an emergency medical condition. The issue in this decision was whether payment had been properly rendered after an undocumented alien's emergency medical condition had been stabilized enough to transfer him.

The case was framed in this manner because the Arizona Health Care Cost Containment System (AHCCCS) denied reimbursement when these patients, all undocumented aliens, were transferred from acute care units to rehabilitative units. AHCCCS based these reimbursement denials on its interpretation of an emergency medical condition under §1903(v). According to AHCCCS, when the patient was transferred no emergency condition existed; therefore, payment was not required for any care rendered after transfer to a rehabilitative unit. All of the patients involved in these cases suffered severe injuries with extensive hospitalizations.

Applicable laws. Arizona law, A.R.S. §36-2905.05(A) provides that undocumented aliens are eligible for AHCCCS coverage "necessary to treat an emergency medical condition as defined in the Social Security Act §1903(v)." Under §1903,

> [T]he "emergency medical condition" means a medical condition (including emergency labor and delivery) manifesting itself by acute symptoms of sufficient severity (including extreme pain) such that the absence of immediate medical attention could reasonably be expected to result in
> (A) placing the patient's health in serious jeopardy,
> (B) serious impairment to bodily functions, or
> (C) serious dysfunction of any bodily organ or part.

42 U.S.C.§1396b(v)(3)(2000) (codifying §1903(v) of the Social Security Act).

Opposing arguments. The hospitals and AHCCCS held conflicting views on payment for the care rendered to these undocumented aliens. The hospitals argued that under §1903(v) once an undocumented alien was admitted, AHCCCS was required to reimburse them until the treating physician determined that the patient and his family caregivers could manage his condition so that adverse consequences were unlikely. AHCCCS contended that when the patient was transferred the patient's condition had stabilized and therefore no emergency medical condition existed.

The pivotal question here was when did an emergency medical condition exist? Once that question was answered, AHCCC's reimbursement obligation could be determined.

Stabilization. The court reviewed the concept of stabilization under prior cases, The Emergency Medical Treatment and Labor Act (EMTALA) at 42 U.S.C. 1395dd(e), and §1903(v). The court determined that (1) the prior decisions in this area were in conflict over the importance that initial injury stabilization played in determining an emergency medical condition, and (2) reliance on stabilization as a determinative factor failed to include a variety of medical conditions and a patient's response to treatment.

The court also reviewed stabilization under EMTALA and §1903(v). EMTALA is concerned with a hospital's need to treat an individual "coming to the emergency room." It utilizes the same definition of emergency medical condition as §1903(v), but has a different view of stabilization. EMTALA requires that a patient be stabilized for transport so that his/her condition will not deteriorate during the time required to facilitate the transfer to another facility. Under EMTALA, stabilization is needed to transfer a patient, however, stabilization does not necessarily exclude an emergency medical condition. Whereas under §1903(v), stabilization is not an express factor to be weighed in the determination of whether an emergency medical condition existed.

Erroneous prior decisions. In its review of these cases, the court determined that the prior holdings were erroneous. According to the court, the tests followed in those cases developed "bright line distinctions" that were impractical. The court found that determining whether an emergency medical condition existed based on (1) stabilization of the initial injury as the determinative factor, (2) looking at the patient unit where the patient was housed, or (3) whether the treating physician determined that the patient and his caregivers can manage his care was impractical. In addition, the court found that neither the plain language nor the intent of §1903(v) envisioned such a bright line distinction between what is and what is not an emergency medical condition. Instead, the court concluded that even though an initial injury may be stabilized that does not mean that the emergency medical condition has ended.

Statutory interpretation. The court stated that in order to determine if an emergency medical condition existed under §1903(v), the focus must be placed on the patient's current condition and whether that condition satisfies the criteria under that statute. The court established a test to be followed. Under this test, the current medical condition must be reviewed to determine whether (1) the initial injury that led to the admission, a condition directly resulting from that injury, or an entirely separate condition, (2) is a non-chronic condition presently manifesting itself by acute symptoms of sufficient severity, and (3) that the absence of medical care could result in one of the three adverse consequences under §1903(v). Furthermore, the court stated that assessment of the acuity or chronicity of symptoms was a question of fact and that the determination of when an emergency condition had ended would require the expertise of health care providers.

Disposition. The Court ruled that the cases be returned to the trial court. There the trial court would determine whether AHCCCS correctly interpreted the relevant law when it applied §1903(v) to the specific facts found by the Administrative Law Judge.

Importance. By this decision, the Arizona Supreme Court facilitated greater access to state reimbursement for hospitals rendering care to undocumented aliens. Such hospitals will now receive revenue previously denied to them.

Does this case have any impact beyond reimbursement for emergency care for undocumented aliens? Probably. Although hospitals in border states like Arizona, have rendered a great portion of nonreimburseable care, they are not the only hospitals in this quagmire. Many healthcare systems are wrestling with uncollected accounts as a direct result of rendering healthcare services to individuals who possess no payment mechanism, be it private insurance or government healthcare programs.

Although this case concerned a state reimbursement statute, Ariz.Rev.Stat. §36-290.05(A) (Supp.1997), that specifically authorized medical coverage for undocumented aliens under certain conditions, hospitals in other states might follow suit and lobby their legislatures to enact specific reimbursement authorization statutes that mandate state payment for care to the uninsured. Then the issue will be how will states, already in a financial morass, take on this additional burden? We will leave that answer to another day and a presidential election. ■

Scottsdale Healthcare, Inc. v. Arizona Health Care Cost Containment System Administration, Ariz. Sup. Ct., CV-02-0190-PR, Aug. 8, 2003,¶370,018

Bill calls for moratorium on specialty hospitals

by Sharon Sofinski

Ohio lawmakers have introduced a new bill that calls for a two-and-a-half-year moratorium on construction of new specialty hospitals. New and existing physician-owned hospitals that filed a notice of intent by September 26, 2003, would be grandfathered in before the moratorium takes effect.

The bill would also prohibit hospitals from dismissing physicians for economic reasons, thus preventing acute care hospitals from dismissing physicians from a specialty hospital, a practice known as "economic credentialing."

The bill replaces earlier legislation that would have prohibited physician investment in specialty hospitals. The state plans to further study any adverse effects specialty care facilities may have on acute care hospitals.

GAO study. The General Accounting Office's (GAO) recent study on specialty hospitals concluded that they "pose a significant and growing threat to full-service community hospitals." The study found that:

- specialty hospitals are a fast-growing segment;
- seventy percent of specialty hospitals are physician-owned; and
- patients treated in specialty hospitals are less ill than those treated in acute care hospitals.

Physicians oppose the proposed moratorium, while hospitals oppose the proposed ban on economic credentialing. A representative from the Ohio State Medical Association questions the need for the bill, saying his group opposes the moratorium "because there is no proof that specialty hospitals have economically harmed acute care hospitals."

According to the Ohio Hospital Association (OHA), the bill "seeks to stop a proliferation of physician-owned limited-service specialty hospitals in Ohio before they cause problems already experienced in other states." The OHA is concerned that since physicians will receive incentives to hand-pick healthier patients, more profitable services will be cut from acute care hospitals, making it more difficult for those hospitals to provide critical care.

The new bill was introduced by the Ohio House Health and Family Services Committee. The full text of the bill is at http://www.legislature.state.oh.us/bills.cfm?ID=125_HB_71. The OHA's press release is at http://www.ohanet.org/media/news_release/2003/gao051601.htm. Text of the GAO study is at http://www.gao.gov/new.items/d03683r.pdf. ■

CCH Chicago Bureau, September 3, 2003

Operations

EHR: Standards on the horizon

by Geraldine S. Stroka, J.D., R.N., M.S.N.

Advocates for electronic health records (EHR) standards may not have to wait very long. The Secretary of Health and Human Services (HHS) recently requested that two organizations, Health Level 7 (HL7) and the Institute of Medicine (IOM), spearhead the effort to develop voluntary EHR functional model standards. In addition, HHS requested that IOM deliver a report on the progress of this project by September 1, 2003.

Project overview. Although the need for EHR standards has been acknowledged throughout the healthcare community, it has been difficult to establish them. This fast-track project required enormous resources and cooperation among many public and private healthcare bodies, especially HL7 and IOM. HL7, a not-for-profit American National Standards Institute accredited standards developer, provides a consensus-based process for standards development. The Special Interest Group of HL7 had long recognized the need for a common industry standard for EHR because it believed that these standards would improve quality and reduce the cost of care while providing better access to clinical

continued on page 8

data. The IOM, established in 1970 by the National Academy of Sciences to act as an advisor to the federal government, was already at work on patient safety data standards when it was asked to lead the EHR project.

The proposed standards, in the form of an IOM Letter Report, were released on July 31, 2003. The standards were "largely based" on plans developed by two other healthcare groups, the Healthcare Information and Management Systems Society and eHealth Initiative. (See the August 13, 2003 edition of iHealthBeat found at http: ihealthbeat.org). The EHR model will have two axes, functions and care settings. The functional axis will have essential, desirable and optional EHR functions across all care settings (e.g., inpatient, ambulatory). IOM will recommend the high-level care-related functionalities for several care settings.

IOM Report. The Letter Report entitled, "Key Capabilities of an Electronic Health Record System," reflects the charge given to IOM—to define the care settings. IOM considered the potential uses and users in developing the core functionalities for EHR systems. It determined that EHR systems uses are primary—supporting the delivery of personal health services, including the delivery of care, care management, care support and administrative processes, or secondary—education, regulation, clinical research, public health and homeland security. The users of this information are both institutional (e.g., hospitals, accrediting organizations) and individual (e.g., clinicians, patients).

IOM identified key EHR functionalities in four care settings—hospital, ambulatory care, nursing home, and care in the communities (the personal health record). IOM determined that a key functionality must (1) improve patient safety; (2) support the delivery of effective patient care; (3) facilitate management of chronic conditions; (4) improve efficiency; and (5) be feasible to implement. Although each functionality may not fulfill all five criteria, when combined as a part of an EHR system, the core functionalities should address all criteria.

The IOM Committee also determined that the core functionalities fell into eight categories. These categories were: (1) health information and data; (2) results management; (3) order entry/management; (4) decision support; (5) electronic communication and connectivity; (6) patient support; (7) administrative processes; and (8) reporting and populations health management.

EHR implementation. Healthcare organizations cannot make the leap from paper medical record systems to comprehensive EHR systems overnight. Instead, IOM estimates that it will take seven years or more for most providers to achieve this goal.

To assist healthcare organizations, IOM divided this seven-year transition phase into three periods, each with specific goals. During 2004-2005, IOM assumes that providers will focus on (1) capturing essential patient data already found in the electronic format, such as laboratory results; (2) the acquisition of currently available software capable of limited decision support (e.g., order entry); and (3) the generation of reports required by external quality organizations. For the period of 2006-2007, IOM envisions that providers' EHR systems should (1) allow capture of defined sets of health information, (2) incorporate a set of decision support functions (e.g., clinical guidelines); and (3) support the exchange of basic patient care data and communication among care settings within a community. In the final period, 2008-2010, the IOM Committee believes that some health systems will possess fully functional, comprehensive EHR systems. This extensive report, including a table listing the eight key EHR system capabilities according to both the care setting and the time frame, is available at http://www.books.nap.edu/html/ehr/NI000427.pdf.

Standards by consensus. A national standard for EHR, as outlined in the IOM report, will affect many healthcare stakeholders. Therefore, the EHR Collaborative, a group of healthcare-related providers and organizations, including the American Health Information Management Association, has sponsored nationwide open forum meetings during August 2003 to get interested parties' input on these EHR model standards. (See http://www.ehrcollaborative.org/.)

After the public meetings have ended, EHR collaborative officials will post a report on its Web site. HL7 will solicit votes on the proposal until September 5 and review the final voting later in September. If the standards pass, they will become effective with a four-month provisional period. After that period has ended, HL7 members will take a final vote. (See Aug. 12, 2003 *Modern Physician* at http://www.modernphysician.com/.)

Importance. Although this EHR system project is a great move forward, as the IOM report states, this is just step one in a two-step process. HL7 will take its next step in the project—incorporating these core functionalities into the model and further specifying each functionality along three dimensions: (1) developing a functional statement or definition; (2) establishing a rationale for the functionality; and (3) establishing a compliance metric or test.

The result of this EHR system project is of extreme importance to healthcare organizations. Hopefully, EHR systems will result in better, safer, and cheaper healthcare for more people. Safety and quality of care are foremost in the minds of all of the participants in the healthcare area—patients, physicians, hospitals, employers, accrediting agencies, and the United States government.

Compliance officers have an enormous stake in the implementation of EHR systems in their organizations. Depending on their specific organizational structure, compliance officers are assuming additional roles including performance improvement and quality initiatives. EHR systems should assist healthcare professionals in accessing critical patient data and thereby improving the quality of care rendered. Compliance officers need to review the IOM report and gauge their organizations' progress against the goals for EHR systems set forth in that document. ■

CCH Chicago Bureau, August 21, 2003