CCH Health Care Compliance LETTER

Volume 13, Issue 2 health.cch.com January 26, 2010

OIG: disclosure of adverse events limited

The Office of Inspector General (OIG) found that public disclosure of information about adverse events was limited, according to its review of 17 state adverse event report systems, eight Patient Safety Organizations overseen by the Agency for Healthcare Research and Quality (AHRQ), and the Centers for Medicare & Medicaid Services (CMS). An "adverse event," also referred to as a "never event," refers to harm to a patient resulting from medical care or harm that occurs in the healthcare setting. Publicly disclosing adverse event information has the potential to educate healthcare providers about the causes of events, possibly leading to improvements in patient safety and assisting patients when making decisions about their care.

Varying extent of disclosure among state systems. State systems receive information about the adverse events and the names of the hospitals. However, systems differ in a variety of ways, including whether reporting was voluntary or mandatory, how information about events was reported, and the types of events reported. State systems also differ on the criteria used to define adverse events, the amount and type of information submitted about patients, and whether hospitals' submissions included information about the causes of events.

Among the entities reviewed, seven state systems disclosed more extensive information about the causes of adverse events and prevention strategies than the other state systems. Disclosures by the seven systems were based on multiple reports of similar adverse events, and included analyses of their causes, actions taken by the hospitals to correct identified vulnerabilities, strategies to reduce the risk of events occurring, and demonstrated improvements by hospitals.

Three other state systems disclosed less extensive information about the causes of the adverse events and prevention strategies. These systems disclosed either information about individual events or lists of events compiled from submitted hospital reports. For example, two systems posted information about individual events, such as event type and date, but did not disclose an analysis of the cause of the adverse events. The remaining system listed all reported corrective actions that hospitals anticipated making, such as planned training, but did not identify the adverse events that precipitated the planned actions.

AHRQ. The Agency for Healthcare Research and Quality (AHRQ) is implementing a program to collect national adverse event information. Hospitals may voluntarily submit adverse event information to Patient Safety Organizations (PSO). In turn, PSOs may provide hospitals with analysis and recommendations for improving patient safety and quality of care. Examples of organizations that have sponsored a PSO include hospital associations, hospital chains, existing patient safety consultant groups, and newly created organizations.

continued on page 2

Wolters Kluwer Law & Business

AHRQ anticipates creating the Network of Patient Safety Databases (NPSD) to provide an evidence-based management resource for providers, patient safety organizations, and other entities. PSOs will submit adverse event information received from hospitals to the NPSD, which will allow AHRQ to receive and publicly disclose non-identifiable adverse event information.

Once the NPSD is operational, the Patient Safety Act requires that the data be used to analyze national and regional statistics, including trends and patterns of reported adverse events, and to generate two public reports on: (1) effective strategies for reducing medical errors and increasing patient safety, and (2) trend analysis results. The initial NPSD data is estimated to be available for analysis and disclosure in early 2011.

CMS. CMS uses hospital claims data to identify certain adverse events called hospital-acquired conditions. CMS has required that hospitals assign a present on admission (POA) indicator to each diagnosis for inpatient Medicare claims. The POA indicator differentiates diagnoses that were hospital-acquired from those that were present on admission. Under the Deficit Reduction Act of 2005 (PubLNo 109-171), CMS was required to select hospital-acquired conditions for which hospitals would not be paid higher Medicare reimbursement. CMS has since selected ten categories of conditions for the Medicare hospital-acquired condition policy, and presently denies hospitals higher payment for Medicare admissions complicated by the ten conditions.

CMS officials indicated to the OIG that CMS is considering posting the incidence of hospital-acquired conditions on its Hospital Compare Website, which presently includes other quality measures about hospitals. CMS may also publicize results from an ongoing evaluation regarding the Medicare hospital-acquired conditions policy, its effects on Medicare reimbursement, utilization, quality, patient safety, and any unintended consequences.

Medicare claims data, however, lack information about the causes of hospital-acquired conditions or prevention strategies. CMS officials acknowledged that supplemental information about the circumstances surrounding a hospital-acquired condition could facilitate understanding of causes and development of prevention strategies. Toward that end, CMS is considering combining hospital-acquired condition data with data from other systems.

Patient privacy. Every entity reviewed by the OIG had patient privacy protections in place that varied in scope. Five state systems did not collect any patient identifiers, such as patient name or address. As a result, these state systems cannot disclose such information. Among the remaining 12 state systems reviewed, there were no instances in which patient identifiers were disclosed publicly. Instead, most publications referred to patients in ways that would prevent identification of patients, although some publications contained details that could be used to identify a patient. The possibility of compromised privacy is exacerbated in circumstances where the patient lives in a smaller community and the media reports on the potentially identifying details. ■

OIG Report, No. OEI-06-09-00360, Jan. 5, 2010

Immediate jeopardy finding fails due to lack of fact-finding specific analysis

A Department Appeals Board (DAB) order upholding the finding of an immediate jeopardy level violation and the imposition of $3,500 per day civil money penalty (CMP) against a skilled nursing facility (SNF) was vacated by the Eighth Circuit Court of Appeals because the DAB's finding was based on pure speculation and not supported by substantial evidence contained in the administrative record. The case focuses on the care provided to an 86-year-old female resident in declining health who ultimately died.

State and CMS action. The Arkansas state agency began a complaint and compliance survey of the SNF based on reports of bruising and dehydration. The state agency informed the SNF that its care reflected noncompliance with six federal regulations, resulting in an "immediate jeopardy" condition. After completing its survey, the state agency recommended that the Centers for Medicare & Medicaid Services (CMS) take enforcement action against the SNF and impose CMPs of $3,500 per day for the six immediate jeopardy violations, plus an additional $350 per day "until the facility is in substantial compliance."

CMS agreed with these recommenda-

continued on page 3

CCH Health Care Compliance Letter

Portfolio Managing Editor
Pamela K. Carron, J.D., LL.M

Coordinating Editors
Susan Smith, J.D., M.A.
Harold M. Bishop, J.D.
Kristine Chung, J.D.

CCH Washington Bureau
Paula Cruickshank
SEC–Peter Feltman
Tax–Jeff Carlson, Steve Cooper, Chandra Walker

Designer
Laila Gaidulis

Requests for information about article submission and comments from readers are welcome and should be directed to Susan Smith at susan.smith@wolterskluwer.com, Tel. 847-267-2780, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Health Care Compliance Letter is published 24 times a year by CCH, a Wolters Kluwer business, 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 Health Care Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

Quality of Care (cont.)

tions and imposed CMPs of $3,500 per day for two days and $350 per day for a period of approximately one month. The SNF conceded the $350 per day sanction, but filed an administrative appeal of the six immediate jeopardy determinations.

ALJ hearing. An administrative law judge (ALJ) decided the appeal on the administrative record. Although the SNF challenged all six immediate jeopardy findings, the ALJ upheld the $3,500 per day penalty on the sole ground that the SNF committed immediate jeopardy violations when several members of its staff observed bruises on the resident for a three-day period and did not investigate the source of these injuries during that same three-day period. The administrative record is clear, however, that the bruises upon which the ALJ based its decision were not observed during the three-day period alleged, but on the morning the resident was transferred to a hospital emergency room with far more serious changes of condition that proved to be the onset of her demise. The ALJ also failed to address the other five immediate jeopardy level deficiencies.

DAB review. On appeal, no doubt realizing the factual flaw in the ALJ's analysis, the DAB affirmed the ALJ's finding of failure to investigate, not based on staff observations of bruising during the three-day period, but on a statement of possible abuse made by a doctor at the hospital after transfer. The DAB also concluded that the ALJ's failure to consider the other five immediate jeopardy violations was immaterial to the case.

Judicial review. The Eight Circuit Court of Appeals found that the state agency and CMS based their immediate jeopardy level charges on six interrelated deficiencies, not based on the failure to investigate bruises observed during the three-day period prior to transfer to the hospital emergency room. The ALJ and the DAB, in effect, convicted the SNF based on a violation not charged, yet the DAB made no fact-specific analysis of the immediate jeopardy issue and cited no facts raising an inference that the SNF's failure to investigate the doctor's statement more promptly or thoroughly increased the risk of abuse. As a result, the DAB's order of immediate jeopardy and imposition of a $3,500 per day CMP was vacated. HHS was also directed to expunge all references to findings of immediate jeopardy level noncompliance by the SNF in HHS and CMS records that are accessible by any means to the public and ensure that the state survey agency does the same. ■

Grace Healthcare of Benton v. CMS, 8th Cir., Dec. 21, 2009, Health Care Compliance Reporter, ¶800,801

Fraud and Abuse

Coding confusion creates jury question in *qui tam* action

The evidence in a *qui tam* action against a medical supplier for submitting improperly coded bills to Medicare and Medicaid showed confusion existed over the proper billing codes and thereby created a jury question as to whether the supplier acted "knowingly" or with "reckless disregard of the truth or falsity" of the claims submitted. A second allegation that the supplier altered prescriptions to call for a more expensive brace in order to receive higher reimbursement was also a question for the jury to decide with regard to all of the government claims except a single count to which the supplier previously pled guilty to in a criminal proceeding.

The supplier was a corporation in the business of supplying durable medical equipment, including back braces. The defendants in the civil *qui tam* (whistleblower) action include the president of the corporation and his wife, who worked for the corporation in a variety of functions, including insurance biller. The back brace in question is called the "System-Loc." The corporation provided 734 of these braces to patients and billed government insurance with an erroneous code that resulted in $874.04 in reimbursement per brace. The government contended that the use of the proper billing code would have resulted in a reimbursement of only $509.22 per brace.

Criminal proceeding. The president of the corporation pled guilty to one misdemeanor criminal count of altering a single back brace prescription which was submitted to Medicare in support of reimbursement. The corporation pled guilty to a felony for the same act but related to a different prescription. All other charges were dropped. The president paid a $100 fine and surrendered the contents of a Medicare escrow account, totaling

continued on page 6

Understanding HITECH – Regulations and Risks

Eric Nelson, CIPP

With most of the provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act scheduled to take effect on February 18, 2010, this timely article is designed to help health care providers benefit from the financial incentives available from the use of qualifying electronic health records and to comply with new requirements and restrictions regarding privacy and security, disclosure, accounting, marketing, and security breach notification.

Background

According to the Los Angeles Times, more than 120 workers at the UCLA Medical Center looked at celebrities' medical records and other personal information without permission between January 2004 and June 2006.

State public health officials reported that 127 workers peeked into celebrities' medical records without permission, leading to several firings, suspensions and warnings. The violations included the patient records of Farrah Fawcett, Britney Spears, California First Lady Maria Shriver and other celebrities.

The report also detailed the case of one employee who looked at the records of about 900 patients "without any legitimate reason" and viewed Social Security numbers, health insurance information and addresses, from April 2003 to May 2007.

In July of 2009, the LA Times reported that the Kaiser Permanente hospital in Bellflower, CA was fined $187,500 for failing a second time to prevent unauthorized access to confidential patient information. State officials said Kaiser Permanente Bellflower Medical Center compromised the privacy of four patients when eight employees improperly accessed records.

According to the article, the hospital was previously fined $250,000 in May for failing to keep employees from snooping in the medical records of Nadya Suleman, the woman who set off a media frenzy after giving birth to octuplets in January 2009. The fine was the first penalty imposed and largest allowed under a new state law, AB 1298, enacted in 2008 after the violations of privacy at UCLA Medical Center.

California was the first state in the country to pass a data breach notification law with the passing of AB 1298, again leading the nation in privacy by expanding the scope of protecting confidential computerized information to include medical and health information. Approximately 46 states have since implemented legislation relating to the protection of an individual's personal information.

ARRA and Electronic Health Records

On February 17, 2009, the American Recovery and Reinvestment Act (ARRA) (PubLNo 111-5), commonly referred to as the Recovery Act, was signed into law by President Obama. The ARRA includes the Health Information Technology for Economic and Clinical Health (HITECH) Act, which provides over $19 billion to help the healthcare industry streamline healthcare and reduce costs through the use of health information technology.

The ARRA provides financial incentives through the Medicare Part B program to help physicians purchase and implement qualifying electronic health records (EHRs) in a meaningful way. Medicare physicians who implement and report meaningful use of EHRs in 2011 will be eligible for an initial incentive payment up to $18,000 and payments in subsequent years with a maximum incentive payout of $44,000 (see chart below). Incentive payments will be reduced in subsequent years, eventually phasing out in 2016.

Physicians who do not use an EHR system before 2015 will not receive any incentive payments and are subject to a reduction in Medicare reimbursements by one percent in 2015, two percent in 2016, and a minimum of three percent in subsequent years.

EHR – Medicare Incentives Schedule for Physicians

Incentive Payment Year	2011	2012	2013	2014	2015
2011	$18k	-0-	-0-	-0-	-0-
2012	$12k	$18k	-0-	-0-	-0-
2013	$ 8k	$12k	$15k	-0-	-0-
2014	$ 4k	$ 8k	$12k	$12k	-0-
2015	$ 2k	$ 4k	$ 8k	$ 8k	-0-
2016	-0-	$ 2k	$ 4k	$ 4k	-0-
2017 +	-0-	-0-	-0-	-0-	-0-
Total	$44k	$44k	$39k	$24k	**-0-**

Privacy and Security Requirements

The HITECH Act was intended to provide assurance to the public that the privacy and security of their patient information is protected. The HITECH Act significantly expands the scope of the HIPAA Privacy and Security rules, including civil and criminal penalties, to business associates – e.g., entities providing services to health care providers, health insurers and other HIPAA "covered entities (CEs)."

Currently, business associates must sign a contract with a covered entity that requires certain HIPAA provisions by contract. The new legislation will obligate a business associate by law to follow all HIPAA security provisions and not just the minimum included in current business associate contracts.

The HIPAA Security Rules relating to administrative, physical and technical safeguards of electronic protected health information (PHI) (plus new security requirements under the HITECH Act that apply to covered entities) now apply directly to business associates in the same way that those standards apply to covered entities.

Non-covered HIPAA entities, such as Health Information Exchanges, Regional Health Information Organizations, and personal health record (PHR) vendors are now required to have business associate agreements with covered entities (including physicians) if they provide the electronic exchange of patient health information.

Additional provisions of the HITECH Act

Increased enforcement and penalties. The legislation substantially increases the civil penalty amounts based on the level and intent of a breach of privacy, e.g., whether the violation was made without knowledge; due to reasonable cause and not willful neglect; or due to willful neglect. The tiers of penalties include:

- Violations determined to be made without knowledge: Penalties start at $100/not to exceed $25,000 per calendar year.
- Violations based on reasonable cause: Penalties start at $1,000/not to exceed $100,000 per calendar year.
- Violations based on willful neglect: Penalties start at $10,000/not to exceed $250,000 per calendar year.
- Violations based on willful neglect and not corrected: Penalties start at $50,000/not to exceed $1,500,000 per year.

The legislation requires a formal investigation and imposition of civil monetary penalties for any violations due to willful neglect. While many of the HITECH final rules are not effective until after February 17, 2010, the provisions on increased penalties were effective immediately.

Lastly, the legislation also gives state Attorney Generals clear and explicit authority to enforce the HIPAA rules on behalf of their residents; permits civil action against an individual or employee that obtains PHI without authorization; and requires the HHS to conduct periodic audits of both covered entities and business to ensure HIPAA compliance.

Disclosure restrictions. Under the HITECH Act, an individual can request that their health care provider not disclose information to an insurer for "payment or health care operations" if the provider has already been paid in full by the individual.

Accounting requirements. The HITECH Act requires a covered entity to provide patients, upon request, an accounting of disclosures of PHI made through the use of an electronic health record if related to treatment, payment or health care operations. If an individual requests an accounting of disclosures, a covered entity must be able to provide disclosure information for the prior three years.

New marketing rules. The HITECH Act prohibits the sale of an individual's PHI without a valid authorization from an individual except in limited circumstances relating to public health activities, research, treatment, the sale or merger of a covered entity, payment to a business associate for services, providing an individual with a copy or access to their PHI or any other activity deemed necessary and appropriate by the Secretary of HHS.

Limited data sets – minimum necessary. The HITECH Act imposes a new requirement to the "minimum necessary" standard, specifically, requiring a covered entity to limit uses, disclosures and requests for PHI to a "limited data set," or if more information is needed, to the minimum necessary amount of PHI to accomplish the intended purpose of the use, disclosure or request.

Security breach notification. Possibly the most significant of the new rules, the HITECH Act requires that covered entities must notify each patient whose *unsecured* PHI has been, or is reasonably believed by the covered entity to have been accessed, acquired, used or disclosed as the result of a breach. While previous HIPAA security requirements applied only to electronic health information, the HITECH rules apply to any form or medium of PHI. The breach notification requirements apply not only to disclosures to third parties, but to unauthorized internal access to PHI.

The regulations require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach "without unreasonable delay and in no case later than 60 calendar days after discovery." The 60 day clock starts on the first day that the breach is discovered by any employee or member of the workforce or on the first day that such a person reasonably should have known of the breach.

Business associates are now required to notify the covered entity of a security breach not later than 60 days after discovery of the breach, which the covered entity in turn will notify the affected individuals. If a breach affects *500 or more* individuals, covered entities are required to provide a notice in prominent media outlets in the immediate area as well as notify the Secretary of HHS, which will post the name of the breaching entity on its public website.

For breaches involving *fewer than 500* individuals, covered entities are required to maintain a log of such breaches and to notify the Secretary on an annual basis. In any case, a covered entity is required to provide notification to any individual whose PHI has been determined to have been breached.

Exceptions to notification requirements include the "unintentional or inadvertent use of disclosure by employees or unauthorized individuals with the same facility."

The Act also requires "vendors of personal health records" and "PHR related entities" to notify their customers of any breach

of unsecured, individually identifiable health information as well as the Federal Trade Commission (FTC). A PHR related entity is defined as an entity that (1) offers products or services through the website of a vendor of personal health records; (2) offers products or services through the websites of HIPAA-covered entities that offer individuals PHRs; or (3) "accesses information in a personal health record or sends information to a personal health record."

HITECH Effective Timeframes

Most of the provisions of the HITECH legislation take effect February 18, 2010; however, the obligation to notify applies to all breaches that are discovered on or after September 15, 2009, and increased penalties for HIPAA violations are effective immediately.

HITECH Challenges and Preparation

A November 2009 Health Information and Management Systems Society (HIMSS) Analytics Report, commissioned by ID Experts, surveyed approximately 176 senior IT executives, chief security officers, chief medical information officers, chief privacy officers as well as vendor organizations that have business associate relationships with healthcare organizations. Some of the key findings of that report include:

- One-third (31 percent) of hospitals reported having a data breach at their organization in the last 12 months, despite almost all (91 percent) having conducted a risk assessment and taken actions to address identified risks and gaps.
- Business associates are generally unprepared to meet the new HITECH data breach-related obligations. Over 30 percent of business associates surveyed did not know the new HIPAA privacy and security requirements have been extended to cover their organizations.
- Eighty-five percent of hospitals indicated they will take action to protect their patient data that are held by a business associate, while a full 39 percent of business associates admitted they did not know what actions hospitals are taking. In addition, business associates were unaware that 47 percent of hospitals would terminate their contracts for violations.

The risks and challenges associated with the HITECH Act are not going away and in fact, enforcement will continue to be more significant and substantial. Steps to prepare for HITECH compliance include:

(1) Identify compliance requirements specific to your organization.
(2) Perform a risk assessment that includes an inventory of PHI assets, including a thorough understanding of how PHI is collected, managed and shared as well as how it is stored, accessed and secured.
(3) Identify and prioritize high risk areas and revise existing privacy and security policies and procedures to address these risks and meet compliance requirements.
(4) Ensure employees and third parties receive privacy and information security training and are constantly aware of their responsibility to protect a patient's personal health information.
(5) Review existing relationships between covered entities and business associates and develop a contracting and compliance strategy.
(6) Develop an effective breach mitigation, detection and response plan that includes internal staff as well as third parties that collect, manage and share PHI.

Summary

The HITECH legislation increases the challenges of protecting an individual's personal health information, but also presents opportunities to increase efficiencies, lower costs and ultimately raise the level of patient care.

Although some questions remain, the HITECH requirements have generally been defined and enforcement provisions are in place. Health care companies and their business associates need to understand how these requirements apply to their organizations and develop strategies to mitigate the risks and ensure compliance.

Eric Nelson is a Practice Leader with Lyndon Group serving clients that have needs with privacy and information security. He is a Certified Information Privacy Professional (CIPP) and specializes in federal, state and international privacy and information security compliance and breach mitigation. Eric a frequent speaker on the subject of privacy and information security through people, policies and processes, has participated on legislative and regulatory committees and served as an advisor to local and state governments. He has contributed to federal identity theft legislation and developed privacy and information security student curriculum currently used by the University of Illinois. Eric is a member of the Healthcare Information and Management Systems Society (HIMSS), the Association of Contingency Planners (ACP) and an active member of The Privacy Consortium, a collaborative group of leading international privacy experts. For more information visit: www.lyndon-group.com.

approximately $79,279. Because the corporation had been dissolved and had no assets, restitution from the corporation was not awarded. All charges were dropped against the president's wife as part of the plea arrangement.

Civil action. The government brought the current *qui tam* action under the False Claims Act (FCA) based on (1) submission of improperly coded bills in violation of 31 U.S.C. §3729(a)(1), and (2) altering prescriptions to receive reimbursement from government insurance in violation of 31 U.S.C. §3729(a)(2). Prior to trial, the government sought summary judgment against the supplier, its president, and his wife.

Improper coding claims. There is little dispute as to the fact that the supplier submitted false claims to the government. The supplier used billing codes that were different than those required by the national organization that sets the codes. Despite the fact that the billing codes submitted seemed to fit the description of the System-Loc brace, there is no evidence to refute the government's assertion that the proper codes were not used. To prove the claim, however, the government must also show that the supplier submitted the wrong codes "knowingly" or with "reckless disregard of the truth or falsity" of the claims. While this element does not require

continued on page 7

specific intent to defraud, it does require some affirmative showing by the government greater than mere negligence.

To support their claim, the government placed great reliance on a letter allegedly sent to the supplier by the brace manufacturer that identified the proper billing codes for the System-Loc brace. The government also contended that the supplier's failure to take the reasonable step of contacting the manufacturer to verify the correct billing codes is evidence of its "reckless disregard." The supplier's president countered that he used the same coding as his previous employer, who never had his reimbursement challenged. More importantly, the supplier asserted that a Medicare ombudsman told them that their procedures were proper during a site visit. These facts, combined with an apparent general confusion surrounding proper billing codes for back braces, make the "knowing" element a jury question. The government's motion for summary judgment on the improper coding claim was therefore denied.

Falsification of records claim. In support of its claim for falsification of prescription records, the government relied exclusively on the guilty pleas of the president and the corporation in the criminal proceeding. The government claimed the criminal pleas estop (prevent) the president and corporation from denying the elements of numerous claims of altering a prescription. The court, however, found that estoppel only applies to claims which involve the same transaction as in the criminal proceeding. Therefore, the president is only prevented from denying the elements of the single count he pled to and not the remaining counts. As a result, summary judgment was granted to the government on the single claim the president pled to in the criminal action. The remaining claims must be considered by the jury at trial.

Secondly, the court found that the president's wife was not liable under the guilty plea of the corporation because it was not certain whether she was ever an officer of the corporation and all charges against her had been dropped in the criminal action. Summary judgment against the president's wife was denied. ■

U.S. ex. rel. Schaefer v. Conti Medical Concepts, Inc., et. al., W.D. Ky., Dec. 17, 2009, Health Care Compliance Reporter, ¶800,795

Impact of the economy on compliance, HCCA/SCCE survey

The effect of the downturn in economy on compliance budgets and staffing in 2009, and the compliance professional's expectations for 2010, are the subject of a joint survey of The Society of Corporate Compliance and Ethics (SCCE) and the Health Care Compliance Association (HCCA). The joint report, entitled "The Economy, Compliance, and Ethics," was generated from a total of 387 survey responses that were obtained during October and November 2009 from compliance and ethics professionals contained in the SCCE and HCCA databases.

2009 budgets and staffing. According to the survey, by the end of the 2009, 26 percent of compliance professionals reported that their budget had increased and 27 percent reported that their budgets had decreased. At the same time, respondents reported that 24 percent had seen a staffing increase and just 18 percent saw a decrease in staffing.

2010 expectations. For 2010, approximately seven percent of survey respondents anticipate their budgets will increase a great deal, and 26 percent expect a marginal increase. Approximately six percent anticipate a substantial budget decrease and 15 percent expect their budgets to decrease marginally. Only three percent of those surveyed expect a large increase in staffing in 2010, with 15 percent expecting a marginal increase. Likewise, only five percent expect a substantial decrease in staffing and eight percent expect a marginal decrease.

Job security. When respondents were asked if they feel that their job is more at risk than others in their organization, 18 percent felt that their job is somewhat more at risk and seven percent felt that their job was much more at risk. However, when asked how concerned they are about losing their job as a result of the current economy, only 11 percent reported that they are very concerned about losing their jobs and 45 percent said they were somewhat concerned.

Management's perspective. Twenty-three percent of the compliance professionals surveyed reported that management sees compliance and ethics as a very positive asset in helping the organization through the current economic conditions. Another 28 percent reported that management felt compliance and ethics were a "somewhat" positive aspect. Only three percent reported that compliance and ethics were a great hindrance in helping the organization through the current economic conditions.

Perceived risk of failure. Fifty-four percent of respondents anticipated that the current economy somewhat increases the risk of compliance and ethics failures and 33 percent of respondents anticipated that the economy greatly increased the risk of failures. Ten percent thought that the current economy somewhat decreases or does not have a significant impact on the risk of compliance and ethics failures.

Warnings and challenges. The joint HCCA/SCCE report notes that at the 2009 Compliance and Ethics Institute of the SCCE, a Federal Sentencing Commission Member Judge warned attendees not to cut compliance budgets, a warning that was echoed by a Deputy Assistant Attorney General in attendance. The report concludes that companies looking to cut budgets may risk raising a red flag in the eyes of prosecutors and the courts; and may find themselves having to explain why they are cutting compliance spending while competitors are maintaining or increasing their budgets. ■

HCCA/SCCE Joint Survey;The Economy, Compliance, and Ethics; Dec. 2009

Trends

Peer review privilege bars disclosure of physician data and documents

A doctor was not required to produce a number of documents on the grounds that they were protected by the state's peer review privilege. The peer review privilege precluded discovery of documents or any other data generated by any peer review committee engaging in peer review activities.

A peer review committee consists of one or more persons who act as a committee of a specified entity, such as a group medical practice. Peer review activities include activities that relate to matters affecting a health professional's membership on the staff, matters affecting employment, and evaluation of the qualifications, competency or performance of any health professional.

The two individuals who had brought suit against the doctor sought to compel a number of documents from the group medical practice that employed the doctor, including: minutes of the quality management committee (QMC) that discuss the doctor's patients; documents reviewed by the QMC concerning the doctor; documents relating to the board of director's meetings that discuss the doctor's employment; and information provided to the state medical association and state board of medical and osteopathic examiners.

The QMC, board of directors, state medical association and state board of medical and osteopathic examiners fell under the definition of "peer review committee" given that the matters at issue related to the doctor's employment, competency, performance and qualification as a health professional on the staff of the group medical practice. Accordingly, they were barred by the state's peer review privilege. ■

Uhing v. Callahan, D. N.D., Jan. 4, 2010, Health Care Compliance Reporter, ¶800,814

In the News

Connecticut AG sues over patient privacy breach

The Attorney General (AG) of Connecticut has filed suit against Health Net of Connecticut, Inc. (HNC), alleging that HNC failed to secure private patient medical records and financial information involving 446,000 Connecticut enrollees and to promptly notify those endangered by the security breach. HNC had discovered that a portable computer disk drive containing unencrypted protected health information (PHI) had disappeared. It wasn't until six months after the discovery of the breach that HNC posted a notice on its website and sent letters to consumers. The AG is also seeking a court order that blocks HNC from continuing violations of the Health Insurance Portability and Accountability Act (HIPAA) (PubLNo 104-191) by requiring that any PHI contained on a portable electronic device be encrypted. This case is the first action by a state AG involving violations of HIPAA since the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted Feb. 17, 2009, authorized state AGs to enforce HIPAA.

Connecticut Attorney General's Office Press Release, Jan. 13, 2010

CMS posts upcoming demonstration projects

The Centers for Medicare & Medicaid Services (CMS) has posted a number of upcoming demonstration projects it will participate in to test and measure the effect of potential program changes. For 2010, the projects include: (1) the Multi-payer Advanced Primary Care Initiative (conducted by states to make advanced primary care practices more broadly available); (2) the Medicare Imaging Demonstration (to collect data regarding physician use of advanced diagnostic imaging services to determine the appropriateness of services in relation to established criteria and physician peers); and (3) the Federally Qualified Health Center Advanced Primary Care Practice Demonstration (evaluating the impact of the advanced primary care practice model on the accessibility, quality, and cost of care provided to beneficiaries served by Federally Qualified Health Centers). For 2011, CMS will participate in the Medicare Enrollment Demonstration (to evaluate the use of a third-party contractor to conduct Medicare Advantage plan enrollment and disenrollment functions).

CMS Update, Jan. 13, 2009

Will Kindle™ DX settlements impact EMRs?

The Department of Justice (DOJ) has reached three separate settlements under the Americans with Disabilities Act with Case Western Reserve University in Cleveland, Pace University in New York City, and Reed College in Portland, Oregon, regarding the classroom setting use of the electronic book reader, the Kindle™ DX, a hand-held technological device that simulates the experience of reading a book. Alan Goldberg, past president of the Amercian Health Lawyers Association, has questioned if these settlements have implications for the use of electronic medical records (EMRs) and other devices by health care providers. Under the agreements, the universities generally will not purchase, recommend or promote use of the Kindle™ DX, or any other dedicated electronic book reader, unless the devices are fully accessible to students who are blind and have low vision. If the universities use the device, they will ensure that students with vision disabilities are able to access and acquire the same materials and information, engage in the same interactions, and enjoy the same services as sighted students with substantially equivalent ease of use. The agreements extend beyond the Kindle™ DX to any dedicated electronic reading device.

DOJ Press Release, Jan. 13, 2009