CCH Healthcare Compliance LETTER

Volume 6, Issue 20 www.cchgroup.com October 13, 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.

Sticking by HR's own set standards is key to JCAHO compliance

by Judith Tichenor, J.D., L.C.S.W., Contributing Editor

What exactly is the Joint Commission on the Accreditation of Healthcare Organization (JCAHO) standard for measuring age-specific competencies in clinical care staff? How can a hospital be sure that it is storing its HR records in the right way? What do JCAHO standards require to ensure that vendors who provide training on highly specialized equipment are properly credentialed?

These and other questions were the subject of the "JCAHO Boot Camp" offered at the American Society for Healthcare Human Resource Associates (ASHHRA) Annual Conference in Denver on August 16, 2003. Carlos G. Beato, RN, MSN, LNHA, JCAHO surveyor and private consultant, gave the three-hour presentation entitled: "Human Resource Management Survival Techniques."

While every healthcare HR department participating in a JCAHO survey wants to know about specific standards and how to ensure their proper implementation, Beato maintained that much of the survey process lies in the hands of the departments themselves. The key to surviving a survey is twofold, according to Beato. First, set your standards based on the areas JCAHO evaluates, in accordance with your healthcare setting's specific needs. Second, comply with the standards you've set.

At first, this advice may seem so simplistic that it is insulting. Yet, the truth is, according to Beato, one of the main reasons healthcare HR departments get a Type 1 recommendation is due to the fact that HR leaders often set perfectly appropriate standards for their specific hospital's HR needs, but then fail to ensure compliance with those standards. Believe it or not, Beato asserts, in most standards, JCAHO "is not in the business of telling you exactly how to perform your department's activities." That is why JCAHO standards tend to read in a very vague manner. The heart of the matter, said Beato, "is the failure to comply with your own standards once you have established them."

"For example," said Beato, "if you say you are doing regular performance evaluations, and then define the concept of timely performance evaluations as an annual process with a 30-day window allowed to accomplish the task, then the Joint Commission will accept that standard as you have defined it. However, if most of your performance reviews are dated well beyond that 30-day final deadline, you are out of compliance with your own standards." That lack of compliance is liable to land your department a Type 1 recommendation, he added.

Another area that prompted questions was HR recordkeeping. Again, Beato pointed out that where and how you keep employee records is up to you, as long as

continued on page 2

you maintain them in accordance with the federal and state regulations applicable in your locality. Once you have established the policy and procedural standards for recordkeeping, however, you must once again ensure that all HR employees are trained for compliance and are actually following through with the standards you have set. "I can't emphasize it often enough," Beato observed. "Compliance with your own set HR standards is what surveyors are monitoring." Beato indicated that most surveyors look for full compliance for at least a year in existing healthcare organizations, and expect full compliance for at least four months in any new healthcare organization.

The same principle applies to setting standards around outside vendors, associates, and outside trainers or consultants. For instance, the clinical unit of a hospital participates with HR and medical technology equipment vendors in deciding upon the standards for credentialing needed for trainers who come in from various vendors to offer staff training on specialized high tech equipment. Once those standards are set, it is up to both the healthcare HR department and each vendor to cooperate to make sure that every trainer sent by the vendor is also adequately trained on the equipment to meet the credentialing standards of the hospital.

Best practice. Make sure your own HR standards are based not only on applicable federal, state, and JCAHO standards, but are also based on well thought-out and reasonably justified rationales specific to your particular healthcare setting. Document the reasoning and rationale that justifies the standards you have set, and then be sure that HR employees and other healthcare managers involved in HR processes are adequately trained on the policies and procedures that create compliance with your set standards. Finally, perform routine evaluations to ensure compliance with your standards once you have set them, and document the corrective actions taken in any area that has slipped out of compliance. ■

CCH Chicago Bureau, Sept. 12, 2003

Corporate Governance

Sarbanes-Oxley standards apply to nonprofit hospitals

by Catherine Hubbard, MA, Contributing Editor

Nonprofit health care organizations need to take the same precautions as for-profit companies that have to comply with Sarbanes Oxley, according to Jack Spalding Schroder, Jr., of Alson & Bird, Atlanta, Ga. "You're going to be painted with the same broad brush that for-profit public health companies are going to be painted with," he said at the Sept. 21-23 American Health Lawyers Association/Health Care Compliance Association conference in Washington, D.C. "You're not as safe or secure as you might think."

Even though Sarbanes-Oxley (SOX) only applies to for-profits that are registered on the NYSE, nonprofit hospitals and other health care organizations need to comply with the same set of standards, said Schroder. "You need to learn how to adapt to this new era of cynicism about corporate governance." According to a *USA Today* survey last year, the health care industry is the second largest source of financial restatements, he said. "Health care companies have been some of the biggest corporate culprits."

"Nonprofit entities need to pay attention," Schroder said. He suggested compliance officers of nonprofit health care organizations:

- Educate board members.
- Evaluate board composition and look at whether there are too many inside directors. "If you have too many insiders, you may be in for trouble." People who are otherwise employed by the hospital and hospital physicians who receive virtually all of their compensation from the hospital are considered insiders, he noted. He also suggested officers consider imposing term limits on board members.
- Strengthen audit committee powers. The committees should have direct power to hire and fire auditors and to recruit financially-savvy members. Only outside directors should be on the audit committee.
- Compare the nonprofit's conflict of interest policies with the IRS' model policy. "You need to look at that model policy." He added that "If you have a doctor on your board who is compensated in any way by the hospital, he or she cannot

continued on page 8

CCH Healthcare Compliance Letter

Managing Editor
Yvonne Kanak

Coordinating Editors
Raio G. Krishnayya, J.D.
Sharon Sofinski

CCH Washington Bureau
Paula Cruickshank
DOJ, FTC–John Scorza
SEC–Peter Feltman
Health Law–Catherine Hubbard
Tax–Jeff Carlson, David Hansen

Designer
Patrick Gallagher

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.

Unprecedented Medi-Cal fraud sentence announced

by Sharon Sofinski

Surinder Singh Panshi, the head of a massive healthcare fraud ring, has been sentenced to 16 years in prison for defrauding California's Medi-Cal system of more than $20 million dollars. The sentence is the longest for Medi-Cal fraud in California's history.

According to California Attorney General Bill Lockyer, "This unprecedented sentence sends a message that we will use the full force of the law to prosecute those who defraud our state."

Panshi, who was arrested in 2002, was sentenced on four felony counts that include fraud, money laundering, conspiracy, identity theft, tax evasion, and committing acts injurious to public health. In addition to the prison sentence, Panshi must pay the state $2.5 million in restitution and the state's Franchise Tax Board (FTB) $124,000 in back taxes.

The two-year-long investigation of Panshi and his associates was conducted by the California Attorney General's Bureau of Medi-Cal Fraud and Elder Abuse, the FTB, the New Jersey Attorney General's Office, and the U.S. Department of Health and Human Services (HHS). Among the 104 felony charges in the complaint against Panshi were submitting false claims to Medi-Cal and Medicare, identity theft, money laundering, tax evasion, endangering public health, and grand theft.

Sophisticated scheme. Panshi, a former doctor, illegally billed government health programs for tests that were not authorized and were not performed. In more than 15 clinical laboratories Panshi controlled, employees were paid to draw excess blood from unsuspecting patients. Other blood was purchased from drug addicts, runaway children, and the homeless. The blood was then tested, and Panshi billed Medi-Cal using patient information that he had stolen. He stole doctors' identities to create false records showing that they authorized the tests. In addition, Panshi ran a black market for the blood and the stolen identities.

Panshi and his cohorts laundered the money they stole from Medi-Cal and Medicare in a small neighborhood store in New Jersey. Checks issued by the government programs were cashed at the store by people carrying phony identification. Some of the money was also laundered through a laboratory equipment company Panshi used as a front.

"This organized crime ring operated a sophisticated scam in order to fleece the Medi-Cal program out of millions of dollars," Lockyer said.

Compounding these criminal activities, Panshi also neglected to file personal income tax returns for 1998 and 1999 and corporate tax returns in 1999. Although he defrauded the state of millions, he reported less than $300,000 in business income.

The New Jersey Attorney General's office also prosecuted Panshi, and he was sentenced earlier this year to 18 years in prison. He is expected to serve his California sentence first and then return to New Jersey to serve the remainder of that sentence.

Others charged. Among the other defendants in the case are:

- Yakoob Habib, who was sentenced for three years for illegally transmitting money in Anaheim. He has been ordered to pay $60,000 in fines.
- Muhammad Yasin, who received an eight-year sentence for conspiracy to commit healthcare fraud and failure to file a tax return. He has been ordered to pay restitution of $510,519.
- Shazad Ahmen, who was sentenced to three years and ordered to pay $67,000.
- Saeed Ahmed, who was sentenced to 16 months and a $20,000 fine.
- Ron Martin, who was arrested and charged with 41 felony counts, including conspiracy, identity theft, fraud, money laundering, and tax evasion.
- Other defendants in the case have pled guilty and are awaiting sentencing, some have been convicted, some are awaiting charges, and two are fugitives from the law.

The press release from the California Attorney General's Office is at http://caag.state.ca.us/newsalerts/2003/03-107.htm. ■

CCH Chicago Bureau, Sept. 9, 2003

The impact of the Privacy Rules on employers

by Harris Beach, LLP

In this excerpt from the CCH HIPAA Privacy Guide, Harris Beach, LLP, addresses the confusion surrounding the HIPAA Privacy Rules' impact on employers. For more information on the CCH HIPAA Privacy Guide, please visit our online store at http://health.cch.com.

Although the April 13, 2003, deadline for most covered entities to comply with the Privacy Rules has passed, there remains significant confusion about how the Privacy Rules impact employers and what obligations, if any, the Privacy Rules place on employers. In general, there are two ways in which an employer, in its capacity as an employer, may be impacted by the Privacy Rules: (1) sponsoring a group health plan;[1] or (2) maintaining an on-site medical clinic. In addition, many employers whose functions make them a covered entity, or a hybrid covered entity, continue to struggle with the determination of what information they maintain about their employees is protected by the Privacy Rules.

The Employer Sponsored Group Health Plan

Many employers will be affected by the Privacy Rules in their role as sponsor of employee group health plans.[2] Group health plans are, by definition, covered entities under the Privacy Rules.[3] It is important to note, however, that for purposes of the Privacy Rules, the group health plan is considered an entity separate and distinct from the plan sponsor. It is actually the group health plan itself that is the covered entity and not the sponsor of that group health plan.[4] The practical implication of this division may be minimal because the administrative functions which most group health plans perform are performed by employees of the plan sponsor.

Administrative Requirements Relating to Group Health Plans

In determining the administrative requirements the Privacy Rules impose on a group health plan, it is first necessary to determine what type of information the group health plan discloses to the plan sponsor. Once that determination is made, there is a further distinction between the obligations of self insured and fully insured group health plans.

Disclosure of PHI to plan sponsor and amendment of plan documents. With certain limited exceptions, a group health plan is prohibited from disclosing PHI to the plan sponsor without a valid authorization, unless the plan documents are amended to permit such disclosures.[5] Specifically, a group health plan, or an HMO or health insurance issuer with regard to that group health plan, may disclose summary health information to the plan sponsor without an authorization and without amending the plan documents if the plan sponsor requests such summary health information for the purpose of obtaining bids for providing health insurance coverage or for the purpose of modifying, amending or terminating the group health plan.[6] Further, a group health plan may disclose to the plan sponsor whether an individual is participating in a group health plan or whether an individual is enrolled in or has disenrolled from an HMO or health insurance issuer offered by the group health plan without an authorization and without amending the plan documents.[7] Any other disclosures of PHI made to a plan sponsor require either an authorization from the insured or an amendment to the plan documents.[8]

If the group health plan, or the HMO or health insurance issuer with respect to the group health plan, intends to disclose PHI, other than the limited information described above, to the plan sponsor, the group health plan's plan documents must be amended to incorporate provisions to:

1. establish the permitted and required uses and disclosures of PHI by the plan sponsor, provided that such uses and disclosures may not be inconsistent with the Privacy Rules; and
2. provide that the group health plan will disclose PHI to the plan sponsor only upon receiving a certification from the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:
   - not use or further disclose PHI other than as permitted or required by the plan documents or as required by law;
   - ensure that any agents, including subcontractors, to whom the plan sponsor provides PHI received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;
   - not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;
   - report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for in the plan documents of which the plan sponsor becomes aware;

- make available PHI in accordance with the individual access provisions set forth in the Privacy Rules;
- make available PHI for amendment and incorporate any amendments to PHI to which the group health plan agrees and in accordance with the provisions of the Privacy Rules;
- make available the information required to provide an accounting of disclosures in accordance with provisions of the Privacy Rules;
- make the plan sponsor's internal practices, books, and records relating to the use and disclosure of PHI received from the group health plan available to the Secretary for purposes of determining the group health plan's compliance with the Privacy Rules; and
- if feasible, return or destroy all PHI received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when it is no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, the plan sponsor will limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.[9]

In addition the foregoing, the plan sponsor must ensure that there is separation between the group health plan and the plan sponsor. Specifically, the recognition of the plan sponsor and the group health plan as two separate entities is a legal fiction. Therefore, it is very likely employees of the plan sponsor will perform those administrative functions which the group health plan is required to perform. In recognition of this fact, if PHI is to be shared with the plan sponsor, the plan documents must also be amended to:

1. describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the PHI to be disclosed, provided that any employee or person who receives PHI relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in this description;
2. restrict the access to and use by such employees or other persons to the plan administration functions that the plan sponsor performs for the group health plan; and
3. provide an effective mechanism for resolving any issues of noncompliance with the plan documents by persons afforded access to the PHI.[10]

Once the plan documents are appropriately amended, the group health plan may:

1. disclose PHI to the plan sponsor to carry out plan administration functions that the plan sponsor performs;
2. not permit the health insurance issuer or HMO with respect to the group health plan to disclose PHI to a plan sponsor, except as specifically permitted by the Privacy Rules;
3. not disclose and may not permit a health insurance issuer or HMO to disclose PHI to a plan sponsor unless the Notice of Privacy Practices of the group health plan states that PHI may be disclosed to the plan sponsor; and
4. not disclose PHI to the plan sponsor for the purpose of employment-related actions or decisions in connection with any other benefit plan of the plan sponsor.[11]

Administrative obligations of fully insured group health plan. Certain fully insured group health plans are not subject to many of the administrative obligations created under the Privacy Rules. For purposes of this exemption, a fully insured group health plan means a group health plan that: (1) provides benefits solely through an insurance contract with a health insurance issuer or an HMO; and (2) does not create or receive PHI except for summary health information or information relating to whether an individual is participating in the group health plan or is enrolled in or disenrolled from a health insurance issuer or an HMO offered by the group health plan.

First, a fully insured group health plan is obligated to comply with the documentation requirements of the Privacy Rules only to the extent such documentation requirements relate to the amendment of the plan documents. Further, a fully insured group health plan is *not* required to:

1. produce or distribute a Notice of Privacy Practices;[12]
2. designate a privacy official or contact person;
3. produce and implement polices and procedures relating to compliance with the Privacy Rules;
4. train employees with respect to the Privacy Rules;
5. implement administrative, physical and technical safeguards to protect the privacy of PHI;
6. implement a procedure by which individuals may file a complaint with the group health plan with respect to violations of the Privacy Rules;
7. implement a policy relating to sanctions imposed on employees for violations of the Privacy Rules;
8. mitigate the known harmful effect of a use or disclosure of PHI in violation of the Privacy Rules.[13]

Note, however, that a group health plan that provides health benefits solely through a contract with a health insurance issuer or an HMO, but receives PHI in addition to summary health information or information on whether an individual is participating in the group health plan, or is enrolled in or disenrolled from an insurance provider or HMO offered by the plan, is not exempt from the administrative requirements of the Privacy Rules. Further, there are special requirements relating to the Notice of Privacy Practices which apply to fully insured group health plans that receive PHI in addition to summary health information and information regarding participation in the group health plan or enrollment in or disenrollment from an insurance provider or HMO

continued on page 6

offered by the plan. Such group health plans must maintain a Notice of Privacy Practices and must deliver that notice to an individual upon request. There is no requirement that such a group health plan receive an acknowledgement of delivery of that Notice.

Administrative obligations of self-insured group health plan. A group health plan that is self-insured, meaning it does not provide benefits through a contract with a health insurance issuer or HMO, is subject to all of the administrative requirements set forth in the Privacy Rules.[14]

There are special provisions regarding the Notice of Privacy Practices which relate to self-insured group health plans. A self-insured group health plan is required to maintain a Notice of Privacy Practices and, no later than the April 14, 2003 compliance date, were required to have delivered that Notice to each enrollee in the group health plan.[15] Thereafter, the group health plan must deliver its Notice to each new enrollee at the time of enrollment in the group health plan. In addition, each enrollee must receive the Notice of Privacy Practices within sixty days of any material revision to the Notice. Finally, at least every three years, the group health plan must notify its enrollees that the Notice is available to them and how to obtain a copy of the Notice.[16]

Use and Disclosure of PHI by a Group Health Plan

Except for disclosures made to the plan sponsor in accordance with the provisions stated earlier in this article, a group health plan is required to comply with all of the restrictions on the use and disclosure of PHI set forth in the Privacy Rules. Therefore, as a general rule, a group health plan is required to have a valid authorization for all uses and disclosures of PHI, unless such use or disclosure is made for treatment, payment or health care operations purposes or the Privacy Rules contain a specific exception to the authorization requirement for such use or disclosure.

Individual Rights Created Under the Privacy Rule

A group health plan is obligated to afford an individual all of the rights created by the Privacy Rules. Specifically, a group health plan must provide an individual the right to access his or her PHI, the right to request an amendment to his or her PHI, the right to request restrictions on the use and disclosure of his or her PHI, and the right to receive confidential communications.

Employers with On-Site Medical Clinics

On-site medical clinic as "covered entity." Some employers maintain or sponsor employee health clinics. The Privacy Rules may be applicable to medical clinics operated by employers, even if the main function of that employer is not the provision of health care. Whether an employer sponsored health clinic is a covered entity will depend on whether that clinic transmits health information electronically in connection with a standard transaction.[17] If an employer sponsored health clinic conducts electronic transactions, then that employer is a covered entity. Pursuant to the Privacy Rules, however, that employer may designate itself as a hybrid covered entity, in which case only those portions of the employer which perform covered functions will be obligated to comply with the provisions of the Privacy Rules.[18]

Requirements of on-site medical clinic. Once an employer has determined that the medical clinic it sponsors is a covered entity and that employer has designated itself as a hybrid covered entity, the Privacy Rules require that the portion of that employer which performs covered functions comply with all of the provisions of the Privacy Rules. This will require the implementation of a complete program to bring the covered portions of the employer into compliance with the Privacy Rules. It is important to note, however, that only the portions of the employer which perform covered functions, in this case the medical clinic, are required to comply with the Privacy Rules.

One of the most difficult issues raised by the employer's status as a hybrid covered entity is the interaction, and specifically the sharing of PHI, between the covered and non-covered portions of that employer. Perhaps the best way to think about a hybrid covered entity for purposes of compliance with the Privacy Rules is as two separate entities, one of which is a covered entity and the other of which is not. As such, if the medical clinic could not disclose PHI to a person or entity unaffiliated with the employer without a valid authorization from the employee, the medical clinic cannot disclose that same PHI to any other portion of the employer without a valid authorization from the employee. Further, if there is an employee who performs functions for both the covered and non-covered portions of the employer, that employee may not use PHI for the non-covered functions he or she performs unless the PHI is properly disclosed by the covered portion of the employer to the non-covered portion of the employer.

The Employment Records Exception

One of the most confusing aspects of the Privacy Rules for employers is the determination of what information it holds is protected by the Privacy Rules. First, an employer that performs no covered functions is not a covered entity, and no information it maintains is protected by the Privacy Rules.[19] This determination, however, is more difficult for the employer that is a covered entity by virtue of its primary functions or the employer that is a hybrid covered entity because it maintains an on-site medical clinic.

In its capacity as a covered entity, all of the PHI maintained by an employer is protected by the Privacy Rules. In addition to being a covered entity, however, many covered entities are also employers. Therefore, it becomes necessary to distinguish between employment records and PHI. This determination can be blurred when the medical information in question relates to an employee of the covered entity.

continued on page 7

In order to dispel some of the confusion, it is important to understand that the definition of "protected health information" expressly excludes "employment records held by a covered entity in its role as an employer."[20] Further, HHS recognized that an employer is required to have certain medical information in its employment records in order to comply with its obligations under the Family and Medical Leave Act, the Americans with Disabilities Act and other similar laws. In addition an employer may require information relating to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance and fitness for duty tests to be in its employee records.[21]

Although HHS did not include a definition of "employment records" in the Privacy Rules, HHS made clear that the determination as to the applicability of the Privacy Rules to certain records maintained by an employer turns not on the nature of the information contained in the record itself, but rather on why the employer is maintaining such information. To illustrate this point, HHS noted:

> drug screening test results will be protected health information when the provider administers the test to the employee, but will not be protected health information when, pursuant to the employee's authorization, the test results are provided to the provider acting as employer and placed in the employee's employment record. Similarly, the results of a fitness for duty exam will be protected health information when the provider administers the test to one of its employees, but will not be protected health information when the results of the fitness for duty exam are turned over to the provider as employer pursuant to the employee's authorization.[22]

Although areas of confusion are likely to remain, the foregoing general principles should resolve many questions. The key determination turns on why the employer has the information. If the information was properly disclosed to the employer and maintained by that employer as part of an employment record, that information is not subject to the protections of the Privacy Rules. Conversely, if the employer maintains the information due to one or more of the covered functions it performs, such information constitutes PHI and is protected by the Privacy Rules in the hands of that employer. This analysis may result in the information in question being protected by the Privacy Rules in the hands of those portions of the employer that perform covered functions, and not protected by the Privacy Rules when it is in the possession of those portions of the employer that do not perform covered functions, including in the employment record of an employee. Although such a conclusion seems illogical, it is often the proper result under the Privacy Rules.

Stevens L. Ingraham, Esq., James A. Tacci, M.D., J.D., M.P.H, and Justin P. Runke, Esq., of Harris Beach, LLP, are the coauthors of the CCH HIPAA Privacy Guide. Harris Beach, LLP, is a top 250 law firm with offices throughout the Northeast. Since its founding in 1856, it has provided a wide range of legal services for a broad-based clientele. Harris Beach's Health Services Department has been at the forefront of structural changes in the rapidly evolving health care industry. Harris Beach attorneys counsel a wide variety of institutional and individual health care providers, multi-provider organizations, managed care organizations and insurers, and have substantial experience in integrated delivery systems and managed care products. Harris Beach's health services include mergers, acquisitions, affiliations, and reorganizations; general corporate; antitrust; regulatory compliance; operations' medical malpractice defense and risk management advice; labor and employment issues; third party reimbursement; financing services; tax, pensions, and employee benefits; and real estate and environmental issues. They regularly provide compliance advice regarding the privacy and security provisions of Health Insurance Portability and Accountability Act of 1996 (HIPAA) to a wide range of clients, including skilled nursing facilities, physician groups, large corporations and free-standing surgical centers. Their attorneys prepare consents and authorizations, modify business associate contracts and agreements, and perform structural and organizational evaluations for organized health care operations to achieve and maintain HIPAA compliance.

1 For a complete definition of the term "health plan" and all terms defined by the Privacy Rules, see the *CCH HIPAA Privacy Guide*.

2 Examples of group health plans include vision, dental and prescription drug plans, long-term care plans and flexible spending plans. Group health plans which are not covered by the Privacy Rules include disability, liability and workers' compensation plans, life and retirement plans, and cafeteria plans.

3 45 C.F.R. §164.103.

4 67 Fed. Reg. 53207 (Aug. 14, 2002).

5 45 C.F.R. §164.504(f)(1)(i).

6 45 C.F.R. §164.504(f)(1)(ii).

7 45 C.F.R. §164.504(f)(1)(iii).

8 Generally, the existence of an employer sponsored group health plan is evidenced by plan documents.

9 45 C.F.R. §164.504(f)(2)(i)-(ii). Note that many of the required amendments to the plan documents are very similar to the provisions which are required to be included in a business associate agreement.

10 45 C.F.R. §164.504(f)(2)(iii).

11 45 C.F.R. §164.504(f)(3).

12 45 C.F.R. §164.520(a)(2).

13 45 C.F.R. 164.530(k). Self-insured group health plans remain obligated to refrain from intimidating or retaliatory acts and cannot require individuals to waive their rights as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits.

14 45 C.F.R. §164.520(a)(2)(ii).

15 45 C.F.R. §164.520(c)(1)(i)(A). This delivery requirement is satisfied if the Notice is delivered to the named insured of the policy, even if there are one or more dependents covered by such policy. 45 C.F.R. §164.520(1)(c)(iii).

16 45 C.F.R. §164.520(c)(1)(i). Note that there is no requirement that the group health plan receive an acknowledgement of delivery of the Notice of Privacy Practices.

17 For a list of standard transactions, please see the definition of "transaction" in *CCH HIPAA Privacy Guide*, Chapter I-3.

18 45 C.F.R. §164.105(a)(2)(iii)(c). For a complete discussion of hybrid covered entities, please see *CCH HIPAA Privacy Guide*, Chapter I-1(B)(3) and Chapter II-1(A)(1).

19 Note that the determination that information maintained by an employer is not subject to the protections of the Privacy Rules does not imply, and should not be taken to mean, that the information is not subject to other state and federal laws which protect the privacy of that information.

20 45 C.F.R. §160.103.

21 67 Fed. Reg. 53191-53192 (Aug. 14, 2002).

22 67 Fed. Reg. 53192 (Aug. 14, 2002).

Corporate Governance (cont.)

vote on his or her compensation or on anyone else's compensation."

- Document all executive compensation decisions. "My rule is document, document, document."
- Beware of "form" financial covenants in loan and bond documents. "I'll bet you the bank document has been changed to include all these Sarbanes-Oxley requirements," he said, cautioning that the changes will apply to nonprofits. "Do you think they're going to give you a different financial document form, just because you're a nonprofit? No, they're going to give you the same statement," he said.

SOX-type violations land nonprofits in court. As the *Health Midwest* ((2003 WL 328845 (D. Kan. 2/6/03)) and *Banner Health Systems* ((2003 WL 21197257 (S.D. 5/21/03)) cases show, state regulators are getting tough on hospitals, said Schroder. Even though the two cases, taken together, do not form a clear precedent for what might happen in the future, they do indicate that nonprofits must be careful when trying to transfer charitable funds out of state. "If you're a nonprofit corporation, the attorney general in your state thinks your money is his or her money," he said. "If you attempt to use that money for out-of-state purposes, or purposes the attorney general doesn't like, you're going to hear from that attorney general."

The states aren't the only ones getting tough, said Schroder. "The feds are getting tough also." He said the *U.S. v. United Memorial Hospital* case (No. 1:01-CR-238) (W.D.Mich., plea entered 1/8/03) was one of the first criminal actions taken against a hospital – in this case a nonprofit. The hospital pleaded guilty that it knew, or at least should have known, that a physician placed a number of patients at unnecessary risk of harm. In this case, there was evidence that the inaction was due to the fact the physician was responsible for one-third of the hospital's income, Schroder noted.

In *U.S. v. Weinbaum* (No. 03 CR 1587L) (S.D.Cal., filed 6/6/03), is a criminal indictment against hospital and its CEO for its physician recruitment practices. "Everyone does physician recruitment," said Schroder, urging hospitals to pay attention to this case. "The government is now going after violations of the anti-kickback law, and against CEOs personally for negotiating those contracts." In *Weinbaum*, the hospital paid over $10 million for 100 new physicians, or roughly $100,000 per physician. However, he said, the money went to the various groups the physicians were joining, rather than to the physicians themselves. The defendants deny wrongdoing and promise a vigorous defense, Schroder said.

IRS weighs in. The IRS made itself clear in Announcement No. 2002-87, where it said nonprofits need to provide the same verifiable information as for-profits, Schroder said. The IRS is saying that both shareholders and contributors to charities need the same type of reliable information when deciding whether to invest or make a contribution, Schroder noted. ■

CCH Washington Bureau, Oct. 2, 2003

False Claims

Doctor to pay $162,000 to settle False Claims charges

by Sharon Sofinski

Dr. Stephen L. Henry has agreed to pay $162,000.00 to settle charges filed against him under the civil False Claims Act, the office of the U.S. Attorney for the Western District of Kentucky announced on September 2, 2003.

Henry, an orthopedic surgeon and lieutenant governor of Kentucky, was charged with causing bills to be submitted for surgeries at the University of Louisville teaching hospital when he was not present or was not immediately available. The complaint alleged that a "significant number" of the surgeries Henry billed to Medicare and Medicaid were actually performed by residents. The complaint included 44 examples of surgeries for which Henry approved billing claims for his services but was absent from the operating room.

The settlement includes the recovery of $60,378 that Henry allegedly improperly billed to the Medicaid and Medicare programs, plus a significant financial sanction. "The settlement demonstrates that the submission of false claims to these programs will not be tolerated," according to the U.S. Attorney's Office. The settlement is also expected to affect Henry's political future.

The Federal Bureau of Investigation and the U.S. Attorney's Office both participated in the investigation. The U.S. Attorney's press release is at http://www.usdoj.gov/usao/kyw/PressReleases.htm. ■

CCH Chicago Bureau, Sept. 5, 2003