



# Physician Organizations

A Publication of the American Health Lawyers Association Physician Organizations Practice Group

## TABLE OF CONTENTS

**Physicians With Substance Abuse Problems: The Issues Which Face Their Employers**  
*Nicholas Giampetro, Esq.*  
*Jeffrey Rockman, Esq.* ..... 1

**Are Your Employees Covered by the ADA? New Guidance May Say, "No"!**  
*Daniel Peters, Esq.* ..... 3

**Physicians Beware: What Every Physician Should Know About the OIG Compliance Program Guidance for Pharmaceutical Manufacturers**  
*Ann Hollenbeck, Esq.* ..... 5

**Inside Physician Organizations: Avoiding the Predictable—Physician Practice Merger Failure**  
*C. Kay Freeman* ..... 7

**The HIPAA Security Regulations: What Physician Practices Should Be Doing Now!**  
*John Murdoch, Esq.* ..... 9

**Building A "High Performance" Messenger Modeling Engine for Physician Practices**  
*Barney Hebert, JD*  
*Eron Reid, CPA* ..... 19

### Physicians With Substance Abuse Problems: The Issues Which Face Their Employers

Nicholas J. Giampetro, Esquire  
*Nicholas J. Giampetro PA*  
*Baltimore, Maryland*

Jeffrey Rockman, Esquire  
*Serotte, Rockman & Wescott*  
*Baltimore, Maryland*

Many physician practice groups are wrestling with the issue of controlled substance use by physicians who are applicants for positions with or employees of the groups. Dealing with physicians applying for positions with a group is relatively straightforward. Like any other employer, a medical group can require a physician applicant to take a drug test as a condition of employment. Indeed, in today's environment, particularly with certain types of practice groups where exposure to drugs is constant, it would be prudent to require such drug testing as a condition of employment.

Any applicant who fails the drug test, or refuses to take the test, typically would be excluded from further consideration for employment. Because of existing federal and state laws, employers, including medical practice groups, are restricted from inquiring into whether applicants have physical, emotional or mental disabilities. The primary law dealing with this issue is the Americans with Disabilities Act of 1990 (ADA).

Most states and many localities have parallel anti-discrimination laws with respect to disabilities.

Under the ADA, a disability is: (1) A physical or mental impairment that substantially limits one or more of the major life activities of such individual; (2) A record of such impairment; or (3) Being regarded as having such impairment. However, the ADA specifically provides that its protections do not apply to an applicant or an employee who is currently engaged in the illegal use of drugs. Therefore, applicants who test positive on a drug test and are therefore excluded from employment may not assert that they have a disability and are being discriminated against by the employer which rejects the applicant for employment.

Likewise, a medical group can institute a drug testing policy which is applicable to current employees as well. Typically, such plans provide for periodic testing of all employees, testing randomly or suspicion-based testing, i.e., testing an individual when there is a reason to believe that he or she is illegally using drugs.

If the employee physician does test positive, what then should the employer do? Some employers depending on the length of tenure of the employee and the quality of the employee's past performance may opt to give the employee another choice. That is, require the employee to go through a rehabilitation program and stay clean in order to keep

his/her job. During the time of rehabilitation, typically, the employee is suspended. If the employee does not successfully complete the program, he/she is terminated. If the program is successfully completed but the employee when subsequently tested by the employer tests positive, the employee is terminated.

The other option when an employee tests positive is not to give the opportunity for rehabilitation but to terminate the employee immediately. Given that in a medical practice there is a heightened concern about having a physician with impaired abilities on staff, many medical groups opt for the immediate termination of physicians who abuse drugs. If the practice opts to terminate the physician, it is advisable to do so without qualification. That is, the terminated physician should not be led to believe that he will have an opportunity for reemployment some time in the future. The reason for this is explained by an unusual provision in the ADA.

Although as discussed above, current drug users are not protected by the ADA, the ADA does provide protection for individuals (who are otherwise qualified for the job in question) who have successfully completed a supervised drug rehabilitation program and are no longer engaging in the illegal use of drugs, or have otherwise been rehabilitated successfully, and is

*Continued on page 2*



AMERICAN HEALTH LAWYERS ASSOCIATION

Leading Health Law to Excellence through Education, Information, and Dialogue

Physician Organizations © 2003 is published by the American Health Lawyers Association. All rights reserved. No part of this publication may be reproduced in any form except by prior written permission from the publisher. Printed in the United States of America. "This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought."

—from a declaration of the American Bar Association

*Continued from page 1*

no longer engaging in such use. Simply stated, this means that an individual may not be denied employment on the basis that they were a drug abuser in the past. Accordingly, while an applicant for a position may be drug tested for current use, no inquiries may be made with respect to any historic use of drugs; such an inquiry would violate the ADA.

The real quagmire exists with respect to a physician who is terminated for drug use from employment, has completed a rehabilitation program and now seeks reemployment with his/her former employer. If the employer has a policy of not offering reemployment to any employee who was terminated for any reason, one would think that would be a sufficient basis for excluding an employee who was a former drug user as well. However, the propriety of such an exclusionary policy is currently unsettled due to a recent decision by the Federal 9th Circuit Court of Appeals, *Hernandez v. Hughes Missile Systems Company*, 298 F. 3rd 1030 (9th Cir. 2002). In that case, an employee who was fired after testing positive for cocaine successfully underwent a rehabilitation program and then reapplied for employment with his former employer. He was rejected based upon the Company's across-the-board policy of not rehiring employees terminated for cause. The 9th Circuit Court of Appeals overturned the decision of the Federal District Court that had held in the Company's favor and found that the policy against rehiring former employees violated the ADA as applied

to former drug users. The Court stated that if Hernandez was no longer using drugs and had been successfully rehabilitated, he could not be denied reemployment simply because of his past record of drug addiction. The case was vacated and remanded to the 9th Circuit by the United States Supreme Court in a decision issued on December 2, 2003. The Supreme Court took issue with the burden on proof analysis employed by the Circuit Court and directed the 9th Circuit to reconsider its analysis using the appropriate factors. Unfortunately, the Supreme Court did not address the underlying issue of the legality of refusing to rehire someone terminated for drug use in violation of company policy.

Employers will not be able to enforce their "no rehire" policies with assurance until the issue is decided. This could be particularly problematic for medical practices since the potential relapse of a physician into drug use poses a danger not only to himself but to patients whom the doctor treats. One can only speculate whether the 9th Circuit will rule the same way on remand. In any event, currently there is no decisional law invalidating such "no rehire" policies.

An additional issue that arises with respect to rehiring a terminated physician for drug use is the re-credentialing process. If the doctor lost his credentials at any hospital(s) where the medical group has privileges, his reemployment by the group may have little meaning since he would not be able to practice in the hospital(s) at which

the group provides services. If the hospital(s) refuses to re-credential the physician, then the employing medical group may have an additional basis upon which to refuse to continue the rehired physician's employment - his inability to practice.

However, the hospital's failure to re-credential the rehabilitated physician may expose the hospital to liability under ADA. In addition to prohibiting discrimination based upon disability in employment, another portion of ADA prohibits discrimination by a public accommodation. The professional office of a health care provider and a hospital are considered public accommodations. Although this aspect of the ADA is most often interpreted to apply to the use of such facility by the public, i.e., patients, there are both case law authority and interpretive decisions by the U.S. Justice Department that physician staff privileges at a hospital are encompassed within ADA's public accommodation protection. Accordingly, the refusal of a hospital to re-credential a physician solely because a physician used drugs in the past may make the hospital vulnerable to a claim of discrimination by the physician.

Another aspect of the problem is the potential conflict between the ADA and the informed consent doctrine. The informed consent doctrine requires a physician to disclose all risks, benefits, etc. that are material to patient's evaluation of whether to submit to the prescribed treatment. If injury results from the undisclosed risk, lack of negligence on the physician's part is irrelevant.

In several jurisdictions, the reasonable patient is the measure of the degree of disclosure required as opposed to measuring whether the physician acted reasonably and in compliance with a medical standard. Application of this type of standard ends up measuring the reasonableness of the patient's expectations versus the physician's actions. The effect of this standard results in a relaxing of the injured patient's burden of proof, since a sympathetic jury could find that a physician had a duty to disclose in the face of expert testimony to the contrary. Further, some jurisdictions require that physicians disclose non-treatment risks, such as HIV, success rates, malpractice and substance abuse [see *Hiddings v. Williams*, 578 So 2d 1192 (La. 1991); contra *Albany Urology Clinic, P.C. v. Cleveland*, 528 S.E. 2d 777 (Ga. 2000) and *Kaskie V. Wright*, 528 A. 2d 213 (Pa. 1991)]. The *Hiddings* case is particularly troublesome since alcoholism is considered a protected disability under the ADA.

The coupling of the reasonable patient standard for disclosure with the requirement that provider-risk be disclosed may exacerbate the conflict between ADA and state laws and the informed consent doctrine. How does the employer reconcile its duty to patients with its exposure to a claim under ADA and state laws?

Some of these issues will be resolved shortly by the Courts; others, practice groups will have to deal with on a case-by-case basis ultimately deciding based on what is in the best interests of their patients.

## Are Your Employees Covered by the ADA? New Guidance May Say, “No”!

Daniel W. Peters, Esquire  
Husch & Eppenger LLC  
Kansas City, Missouri

### I. Introduction

A recent case decided by the United States Supreme Court may impact the determination of whether physician practices are subject to the Americans with Disabilities Act (ADA) and certain other laws which affect employers based on the number of its employees (such as Title VII of the Civil Rights Act, the Age Discrimination in Employment Act (ADEA), and the Family and Medical Leave Act (FMLA)). In *Clackamas Gastroenterology Associates, P.C. v. Wells*, No. 01-1435, 538 U.S. \_\_\_\_ (Apr. 22, 2003) the Court provided guidance in determining who is an “employee” under the ADA. In its decision, the Court determined that the common-law element of “control” is the principal guidepost that should be followed in making this determination.

The case involved Deborah Anne Wells who worked at Clackamas Gastroenterology Associates, PC, for eleven years and was fired in 1997 because of her disability, described as “a debilitating tissue disorder.” Wells claimed that she was demoted, then forced to resign. Wells sued the clinic under the ADA, which bans discrimination against people with disabilities, alleging that the employer illegally terminated her employment based on her disability, in violation of Title I of the ADA. Title I of the ADA makes it unlawful for a “covered entity”

to “discriminate against a qualified individual with a disability . . . in regard to . . . discharge of employees.” 42 U.S.C. §12112(a). Wells argued that the ADA prohibited Clackamas from terminating her due to her disability.

The Court did not address whether the clinic had discriminated against Wells, but instead focused on whether the clinic was large enough to be covered under the ADA. When Congress drafted the ADA, it decided that it would be inapplicable to certain small businesses. According to the ADA, small businesses are generally defined as having less than fifteen employees. Specifically, an “employer” is not covered by Title I of the ADA unless its workforce includes “15 or more employees for each working day in each of 20 or more calendar weeks in the current or preceding calendar year.” 42 U.S.C. §12111(5)(A). The Clackamas medical group had less than fifteen employees if the physicians were not counted as employees, and over fifteen employees if the physicians were counted as employees. *The question presented to the Supreme Court was whether physicians actively engaged in the corporation’s medical practice as shareholders and directors of a professional corporation are counted as “employees” within the meaning of the ADA.*

The Clackamas group argued that the owners of the business—which included four doctors—were not employees for purposes of meeting the ADA employee threshold rule. The U.S. Court of Appeals for the Ninth Circuit had previously ruled that the physician owners were “employees” and that the clinic

therefore employed more than the fifteen employee threshold and was subject to the ADA.

### II. Court’s Decision

The Court disagreed with the prior decision and in a 7-2 decision held that the common-law element of control is the principal guidepost to be followed in deciding whether the four director-shareholder physicians in this case should be counted as “employees.” Interestingly, the Court determined that the ADA’s definition of employee (“an individual who is employed by the employer”) is completely circular and explains nothing.

Instead, the Court agreed to apply Equal Employment Opportunity Commission (EEOC) guidelines discussing both the broad question of who is an “employee” and the narrower question of when partners, officers, members of boards of directors, and major shareholders qualify as employees, and listed the following six factors as relevant to the inquiry whether a shareholder-director is an employee:

- “Whether the organization can hire or fire the individual or set the rules and regulations of the individual’s work.
- Whether and, if so, to what extent the organization supervises the individual’s work.
- Whether the individual reports to someone higher in the organization.
- Whether and, if so, to what extent the individual is able to influence the organization.
- Whether the parties intended that the individual be an employee, as expressed in written agreements or contracts.

- Whether the individual shares in the profits, losses, and liabilities of the organization.” (*EEOC Compliance Manual §605:0009*).

The Court commented, “The mere fact that a person has a particular title—such as partner, director, or vice president—should not necessarily be used to determine whether he or she is an employee or a proprietor. Nor should the mere existence of a document styled ‘employment agreement’ lead inexorably to the conclusion that either party is an employee.” The answer to whether a shareholder-director is an employee for ADA purposes depends on “all of the incidents of the relationship . . . with no one factor being decisive.”

The Court noted several findings from the trial court that weighed in favor of the physicians being viewed as shareholders and not as employees: (1) they apparently control the operation of their clinic, (2) they share the profits, and (3) they are personally liable for malpractice claims. Nevertheless, the Court did not reach a conclusion on the issue of employment status, because it noted that there might be some evidence in the record that contradicted such conclusions.

### III. Practical Implications

The *Clackamas* case may have some practical implications for physician practices. If the physician practice is a small practice at or near the employee threshold for the ADA or certain other employment related laws, this decision may provide the practice with some added

*Continued on page 4*

Continued from page 3

legal flexibility in making difficult employment decisions. If a practice is not subject to the anti-discrimination laws of the ADA, the group may have additional defenses to employment litigation, or may be able to make difficult employment decisions that would otherwise be prohibited by the ADA with less risk and uncertainty. Keep in mind, some state discrimination laws do not apply the same employee thresholds as their federal law counterparts. In fact, most state discrimination laws have jurisdictional thresholds that are less than fifteen employees, such as Missouri, which has a six employee threshold. It is necessary to check applicable local laws to know what state laws provide.

In a footnote, the Court commented that the meaning of the term "employee" comes into play both (i) when determining whether an individual is an "employee" who may invoke the ADA's protections against discrimination in "hiring, advancement or discharge," and (ii) when determining whether an individual is an employee for purposes of the fifteen-employee threshold. This may mean that based upon the common-law test described in the *Clackamas* case, a physician-shareholder may be found not to be covered by the employment discrimination laws of the ADA, irrespective of whether the practice meets the employee threshold or not. As mentioned above, compliance with certain other federal laws such as the FMLA or ADEA are also based upon having a certain

number of employees, and likely command the same analysis.

According to the Supreme Court's new guidance in *Clackamas* (and similar guidance offered in *Devine v. Stone, Leyton & Gershman, P.C.*, 100 F. 3d 78 (8th Cir. 1996)), to be classified as owners, shareholders must actually have the authority to make management decisions and must share in profits. Medical practices that want to remain under a jurisdictional limit should structure their business operation to show that each shareholder has authority in management decision-making. Professional corporations can keep minutes of votes, be sure their communications or e-mails do not suggest that some shareholders are without authority, and establish records reflecting that each shareholder possesses all the incidents of ownership. For example, a physician shareholder could have the authority, singly or with others, to terminate employees, make decisions on contracts, and so forth. Each of those factors weigh against a physician-shareholder being counted as an "employee" according to the law decided by this case. Of course, there may be other non-employment business reasons why some of these rights or decisions should be limited among the shareholders.

## Physician Organizations Practice Group

*Leadership 2003-04*

### **Michael F. Schaff** **Chair**

Wilentz Goldman & Spitzer PA  
PO Box 10  
90 Woodbridge Center Drive  
Woodbridge, NJ 07095-0958  
Phone: (732) 855-6047  
E-mail: schafm@wilentz.com

### **Charlene L. McGinty** **Vice Chair & Editor**

Powell Goldstein Frazer  
& Murphy LLP  
16th Floor  
191 Peachtree Street NE  
Atlanta, GA 30303-1740  
Phone: (404) 572-6733  
E-mail: cmcginty@pgfm.com

### **Cynthia Y. Reisz** **Vice Chair**

Bass Berry & Sims PLC  
315 Deaderick Street  
Suite 2700  
Nashville, TN 37238-0002  
Phone: (615) 742-6283  
E-mail: creisz@bassberry.com

### **Lisa D. Taylor** **Vice Chair**

St John & Wayne LLC  
2 Penn Plaza East  
Newark, NJ 07105-2257  
Phone: (973) 491-3302  
E-mail: ldt@stjohnlaw.com

## Physicians Beware: What Every Physician Should Know About the OIG Compliance Program Guidance for Pharmaceutical Manufacturers

Ann T. Hollenbeck, Esquire  
*Honigman Miller Schwartz & Cohn LLP*  
 Detroit, Michigan

On April 28, 2003, the Department of Health and Human Services (DHHS) Office of Inspector General (OIG) issued the *Final Compliance Program Guidance for Pharmaceutical Manufacturers* (CPG). This CPG, which was issued in draft form on October 3, 2002, is intended to help companies that develop, manufacture, or sell pharmaceutical drugs or biological products (pharmaceutical manufacturers) identify risky practices and promote compliance with federal healthcare program rules. While the guidance is tailored for implementation by pharmaceutical manufacturers, the nature of the compliance issues described in the CPG potentially implicates hospitals, physicians, and all other healthcare providers that do business with the federal healthcare programs. No one in the healthcare industry, particularly physicians, can afford to ignore it.

While the CPG is somewhat similar to the draft compliance guidance issued in October 2002, it includes expanded discussions of risk areas and additional insights on compliance strategies. As in the draft compliance guidance, the CPG focuses on the three following specific risk areas that are of

current concern and interest to the enforcement community because of their potential for fraud and abuse.

### I. Data Integrity

Because many federal and state healthcare programs establish reimbursement rates for pharmaceuticals using price and sales data furnished by pharmaceutical manufacturers, the knowing submission of false, fraudulent, or misleading information is a violation of federal law under the False Claims Act<sup>1</sup> and potentially the federal Anti-Kickback Statute<sup>2</sup>. All reported prices must accurately take into account price reductions, cash discounts, free goods contingent on a purchase agreement, rebates, up-front payments, coupons, goods in kind, free or reduced-price services, grants, and other price concessions.

### II. Kickbacks and Other Illegal Remuneration

The OIG makes clear its concern about potential kickback schemes between pharmaceutical manufacturers and healthcare providers as it is by far the lengthiest discussion of compliance risks in the CPG. Although the Anti-Kickback Statute ultimately turns on a party's intent, the OIG provides a two-step analysis for determining whether an arrangement presents a significant potential for federal healthcare program abuse. These steps are applicable to a physician's relationship or arrangement with a pharmaceutical manufacturer and are set forth as follows from the physician's perspective. First, the physician should identify any and all compensation or other payment relationships

he/she (including his/her group, partners, employees, employer or agents) has with a pharmaceutical manufacturer to which he/she (or his/her group, partners, employees, employer or agents) is in a position to refer or recommend business payable in whole or in part by a federal healthcare program. Second, the physician should determine whether any purpose of the compensation or other payment relationship may be to induce or reward the referral or recommendation of business payable by a federal healthcare program. In addition, the OIG encourages consideration of the following questions: Does the arrangement skew clinical decision-making? Does the arrangement have the potential to increase costs to the federal healthcare programs, beneficiaries, or enrollees? Does the arrangement have a potential to cause over-utilization? Does the arrangement raise patient safety or quality concerns? The CPG continues by highlighting the following "known areas" of potential risk:

- **Discounts:** reductions in price for pharmaceuticals are allowed, but must be properly reported and managed under the Anti-Kickback Statute safe harbor applicable to discounts.
- **Product Support Services:** support services provided by pharmaceutical manufacturers are allowable so long as they have no substantial independent value to the purchaser.
- **Educational Grants:** grant funding for educational activities is allowed, but funding conditioned on the purchase

of products implicates the Anti-Kickback Statute even if the educational or research purpose is legitimate.

- **Research Funding:** when pharmaceutical manufacturers contract with purchasers of their products to conduct research activities, such relationships should be structured to fit within the personal services safe harbor<sup>3</sup> of the Anti-Kickback Statute (*i.e.*, payments for research services should be fair market value for legitimate, reasonable, and necessary services). Further, research should be supervised by the scientific or grant-making area of the pharmaceutical manufacturer, not by the sales and marketing department.
- **Formularies:** while the OIG recognizes that formularies are a well-established tool for the effective management of drug benefits, it warns that the clinical efficacy and appropriateness of formulary drugs must be paramount to the consideration of costs. Further, the OIG views any payments, whether direct or indirect, to members of formulary committees or to pharmacy benefit managers, as suspect under the Anti-Kickback Statute.
- **Relationships with Physicians:** if gifts, meals, entertainment, etc. are provided to physicians with the intent to generate business to a federal healthcare program, the OIG warns that the Anti-Kickback Statute will be violated despite a legitimate additional purpose (such as physician educa-

*Continued on page 6*

tion). The OIG states that an arrangement must fit squarely within an Anti-Kickback Statute safe harbor to be protected. Those not falling within a safe harbor should be reviewed with the following factors in mind: the nature of the relationship between the parties, the manner in which the remuneration is determined, the value of the remuneration, the potential federal program impact of the remuneration, and potential conflicts of interest.

- **Switching Arrangements:** cash payments from pharmaceutical manufacturers to physicians who switch prescriptions to the manufacturers' products are suspect and in the opinion of the OIG "clearly implicate" the Anti-Kickback Statute.<sup>4</sup>
- **Consulting and Advisory Payments:** fair market value payments to physicians or other healthcare providers for *bona fide* services are unlikely to raise concerns; however, compensating persons to attend meetings in a passive capacity is suspect. Compensation relationships with physicians for services connected directly or indirectly to a manufacturer's marketing and sales activities, such as speaking, certain research, or perception or shadowing services are suspect. In particular, ghost-written papers or speeches implicate the Anti-Kickback Statute. The OIG specifically states that a full disclosure of a conflict of interest will not eliminate the risk of violating

the Anti-Kickback Statute. Physicians should structure relationships with pharmaceutical manufacturers to comply with a safe harbor whenever possible. And, the OIG suggests that physician services arrangements be periodically reviewed to ensure that: the arrangement is set forth in writing, there is a legitimate need for the services, the services are provided, the compensation is at fair market value, and all of the preceding facts are documented prior to payment.

### III. Pharmaceutical Samples

The provision of pharmaceutical samples is a widespread industry practice that can benefit patients. However, the Prescription Drug Marketing Act of 1987<sup>5</sup> governs the use of pharmaceutical samples and *forbids* their sale. According to the CPG, recent government enforcement activity has focused on instances where pharmaceutical samples were provided to physicians who, in turn, sold them to patients or billed them to federal healthcare programs on behalf of patients.

In today's environment of increased OIG scrutiny of corporate conduct and increasingly large expenditures for prescription drugs, healthcare providers should proceed with caution before entering into arrangements with pharmaceutical manufacturers. The CPG can be accessed and printed through the OIG website at <http://oig.hhs.gov/fraud/complianceguidance.html>. An additional helpful compliance resource is the PhRMA Code of Interactions with Healthcare

Professionals, a voluntary code promulgated by the Executive Committee of the Pharmaceutical Research and Manufacturers of America, which became effective July 1, 2002. It is available on PhRMA's website at [www.phrma.org](http://www.phrma.org). The PhRMA Code provides additional guidance for evaluating relationships between pharmaceutical manufacturers and providers. Arrangements that fail to meet the minimum standards set forth in the PhRMA Code are likely to receive increased scrutiny from the OIG and other regulators.

#### Endnotes

- <sup>1</sup> 31 U.S.C. § 3729-33.
- <sup>2</sup> 42 U.S.C. § 1320a-7b(b).
- <sup>3</sup> 42 C.F.R. § 1001.952(d).
- <sup>4</sup> See the OIG's 1994 Special Fraud Alert at 59 Fed. Reg. 65372, Dec. 19, 1994.
- <sup>5</sup> 21 U.S.C. 353(c)(1).

## AMERICAN HEALTH LAWYERS ASSOCIATION

1025 Connecticut Ave, NW  
Suite 600  
Washington, DC 20036-5405  
202-833-1100  
202-833-1105 Fax

[www.healthlawyers.org](http://www.healthlawyers.org)

### PRACTICE GROUPS STAFF

**WAYNE MILLER, CAE**  
Deputy Executive Vice  
President/COO  
(202) 833-0775  
[wmiller@healthlawyers.org](mailto:wmiller@healthlawyers.org)

**EILEEN M. BANTEL**  
Practice Groups Manager  
(865) 458-0643  
[ebantel@healthlawyers.org](mailto:ebantel@healthlawyers.org)

**LAURIE M. GARVEY**  
Practice Groups Coordinator  
(202) 833-0783  
[lgarvey@healthlawyers.org](mailto:lgarvey@healthlawyers.org)

**SARAH MUENZENMAYER**  
Practice Groups Assistant  
(202) 833-0765  
[smuenzenmayer@healthlawyers.org](mailto:smuenzenmayer@healthlawyers.org)

## Inside Physician Organizations: Avoiding the Predictable—Physician Practice Merger Failure

C. Kay Freeman

President

Health Systems Strategies

Atlanta, Georgia

Physician practice mergers are easier to put together than they are to live with. Lawyers representing physicians contemplating a merger should not ignore this fact and its impact on the subsequent success or failure of the merger.

Physicians, driven by declining reimbursement and narrowing recruitment capability, are turning to mergers as a means to sustain current compensation and the opportunity to prosper in an adversarial environment. This is particularly true of physicians in solo or small group practice.

Mergers between physician practices *can* result in reduced overhead expense and *can* strategically position the merged entity to achieve a sustained competitive edge. *Can* is the crucial word. Factually, most physician practice mergers do not achieve their intended objectives. Further, *very few* merged physician groups know or reach their full potential.

Multiple underlying factors limit a merged group's ability to realize its intended objectives and full potential, or worse, can precipitate its subsequent demise. Lawyers representing practices exploring mergers should have a clear understanding of these factors and their adverse impact. Further, lawyers should incorporate strategies for preventing or removing such factors *before* merger documents are executed.

The lawyer's position in physician practice mergers presents an opportunity for them to take the initiative early in the process to identify if one or more of these adverse factors are present and to recommend strategies for removing or minimizing their impact. Lawyers, therefore, could likely decrease the incidence of partial and total merger failure by taking the initiative in identifying and addressing these underlying factors before they become problematic. Underlying factors include those illustrated below:

- **Driving Merger Objective.** Some lawyers' and consultants' view is that the driving merger objective should be *the maximum autonomy permitted* under the regulations governing physician practice mergers. Such views disregard the fact that merged groups whose driving objective is to *integrate to the degree required to achieve their current and future full potential* are better positioned to thrive rather than merely survive in an adversarial practice environment.
- **Resistance to Change.** Physicians have a strong resistance against change not inspired by sustained conflict, crisis, or a federal mandate.
- **Agreements Not Implemented.** Physicians agree to make required changes thinking that they will never *have to actually*

*make them.* The resulting adverse effect is compounded by the failure of lawyers and consultants to identify, address, and dispel this flawed thought process.

- **Failure to Identify Differences.** Physicians, lawyers, and consultants fail to take the time to factually identify and analyze individual practice characteristics and concomitant failure to reconcile differences *before* they enter into a merger.
- **Unmet Expectations.** These are generally caused by the failure to identify each individual physician's *un-communicated* merger expectations and priorities and the failure to turn diversity into realistic, unified, achievable expectations *before* entering into a merger. This can result in conflict caused by the failure to identify each merger participant's short and long term expectations of the other and the failure to reconcile diverse expectations *before* entering into a merger.
- **Approving Internal Agreements After Merger.** Some lawyers and consultants believe that certain internal agreements can be developed and approved *after* entering into a merger. However, this view ignores the reality that it is, in fact, the development and approval process of internal agreements that expose uncommunicated diversity, precipitate conflict, and foster subsequent merger failure.
- **Deficient Merger Organization and Governance Structures.** The use of traditional structures perpetuates the deficiencies and limitations of those structures in the new entity. Vision and strategy skills should be employed to design structures that strengthen a merged group's ability to meet the needs and challenges that are unique to merged groups.
- **Apathy Regarding Merged Physician Interaction.** Physician interaction plays a key role in determining the mergers success or demise. The failure to address the major physician interface issues with practices *before* they merge and the absence of written physician interaction policy, foster dysfunctional and failed mergers.
- **Reluctance to Address Sensitive Issues.** Physicians have an aversion to addressing sensitive issues during merger feasibility and development based on their fear of offending peers and concern about the effect it could have on the pending merger. Likewise, lawyers and consultants might avoid handling and addressing sensitive issues based on their unwillingness to risk offending a client or worse, termination.

Continued on page 8

*Continued from page 7*

- **Deficient/Unrealistic Business Plans.** One key to a successful merger is having a business plan that has been thoroughly thought out and discussed among the parties. A deficient and/or unrealistic business plan can lead to a failed merger.
- **Inadequate Merger Feasibility Process.** This process requires input and review by all parties. This can also lead to the reluctance of physicians, lawyers, and consultants to declare merger incompatibility when feasibility findings indicate strong or irreconcilable incompatibility.
- **Underlying Conflict of Interest.** Conflict of interest issues can arise primarily with consultants' whose underlying objective is to provide post merger administration, accounting, and/or billing services. If this is the case, findings and recommendations presented by the consultant should be carefully scrutinized to rule out compromised objectivity.
- **Weak Merged Group Administration.** Weak administration post-merger can be caused by physicians' tendency to seek administrators inclined to tell them what they want to hear rather than what they should be told. Weak administration should be addressed and strongly advised against early in the merger process.
- **Merger Factors.** The decision to merge is driven by five dominant factors: (i) Fear; (ii) Competitive edge; (iii) Economic survival; (iv) Current trend; and (v) Power. These five factors create both opportunity and risk. The degree of risk or opportunity experienced is determined by:
  - The level of importance lawyers and consultants assign to each factor;
  - Their knowledge regarding each factor's impact on mergers;
  - Their willingness to factually identify which factor(s) applies to the individual practices participating in the merger; and
  - The degree of success achieved in reconciling diversity and neutralizing each factor's adverse effect.
- **The Myth—Presence of Advisors.** Physicians believe that if lawyers and/or consultants are present in the transaction, physicians can meet and through general discussion can identify and resolve their respective concerns and differences. History and experience demonstrate that physicians in the same practice rarely disclose their actual views and thoughts to one another in meetings with or without advisors present. Therefore, it is illogical to assume that they would do so when participating in general discussion with another or multiple practices with or without advisors present.

This myth's effect typically does not emerge until *after* the merger, when physicians discover that *mergers are easier to put*

*together than they are to live with, and that change is a requirement not an option.* Experience further demonstrates that *formal, facilitated structured fact finding sessions* are the most effective way to factually identify, address, and reconcile individual physicians' expectations, views, and concerns.

Physician practice organizations seemingly have learned through their experience with practice management companies that they cannot abdicate their own responsibility for practice economic and operations stability. If true, physicians will take the only path left for them to sustain if not improve current compensation levels and to grasp opportunities when they emerge. This path is consolidation of practice resources through mergers.

This being the case, lawyers representing physician practice organizations should make a conscious effort to delve into the intersanctum of merged groups to become more knowledgeable regarding the challenges merged groups face after the documents are executed and the lawyers and consultants have departed to await the predictable call from the group reporting that they have encountered internal turbulence. In short, doing it right the first time will obviate the incidence and severity of internal turbulence experienced.

## The HIPAA Security Regulations: What Physician Practices Should Be Doing Now!

John P. Murdoch II, Esquire  
*Wilentz Goldman & Spitzer PA*  
*Eatontown, New Jersey*

On February 20, 2003, the federal Department of Health and Human Services (DHHS) adopted final regulations pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to protect patient health information (PHI) maintained or transmitted electronically (HIPAA Security Regulations).<sup>1</sup> The HIPAA Security Regulations require those persons or entities designated as “covered entities”<sup>2</sup> to implement basic safeguards to protect electronic PHI from unauthorized access, alteration, deletion, and transmission.<sup>3</sup> The regulations supercede contrary state law provisions,<sup>4</sup> and as such, establish a minimum level of security.<sup>5</sup>

While the HIPAA Security Regulations will become effective April 20, 2005,<sup>6</sup> such regulations should be closely analyzed under the “mini-security rule” contained in the privacy regulations adopted under HIPAA Privacy Regulations,<sup>7</sup> which requires covered entities to implement appropriate administrative, technical, and physical safeguards.<sup>8</sup> As such, while compliance with the HIPAA Security Regulations is not yet required, the standards in the HIPAA Security Regulations serve as guidance by offering appropriate safeguards that should be implemented by a physician practice that is a covered entity

(Practice), as part of its policies and procedures required under the HIPAA Privacy Regulations “mini-security rule.” Further, the Practice will likely require at least a year to fully analyze the HIPAA Security Regulations, evaluate the Practice, implement the standards, and effectively evaluate the effectiveness of such standards. As such, the Practice should not wait until April 2005 to implement the HIPAA Security Regulations. Instead, it should begin now!

### I. General HIPAA Security Regulations’ Requirements

#### A. Covered Entities

Persons or entities that meet the definition of a covered entity must comply with the HIPAA Security Regulations.<sup>9</sup> Covered entities are defined as:

- health plans,
- healthcare clearinghouses, and
- healthcare providers who transmit any health information in electronic form in connection with a covered transaction.<sup>10</sup>

Such covered transactions include the following:

- healthcare claims or equivalent encounter information,
- healthcare payment and remittance advice,
- coordination of benefits,
- healthcare claim status,
- enrollment and disenrollment in a health plan,
- eligibility for a health plan,
- health plan premium payments,
- referral certification and authorization,

- first report of injury,
- health claims attachments, and
- other transactions that the Secretary of the DHHS may prescribe by regulation.<sup>11</sup>

The definition of a covered entity is the same under the HIPAA Privacy Regulations and the regulations governing standard electronic transaction code sets under HIPAA Electronic Transactions and Code Set Regulations.

#### B. Covered Information

The HIPAA Security Regulations protect the confidentiality, integrity, and availability of electronic PHI.<sup>12</sup> These regulations define electronic PHI as individually identifiable health information that is transmitted or maintained in electronic media.<sup>13</sup>

DHHS has noted an exception to electronic PHI for information not in an electronic format before transmittal.<sup>14</sup> Examples of this exception include information transmitted via a telephone or facsimile (either by voice or a DTMP tone pad). As such, paper-to-paper faxes, person-to-person telephone calls, and messages left on voice mail are excluded from the definition of electronic PHI.<sup>15</sup> Please note that all electronic PHI maintained or transmitted by the Practice is covered under the HIPAA Security Regulations, even if such information is never transmitted to a third party.

### II. Overview

In addition to general requirements, the HIPAA Security Regulations can be broken down into three broad categories including administrative, physical, and technical safe-

guards. In each of these broad categories, various standards exist for ensuring the security of electronic PHI, which are discussed below. Most standards have at least one implementation specification that is either “required” or “addressable.” While required specifications must be adopted by the Practice by April 21, 2005, the Practice must conduct the following analysis with respect to addressable specifications:

- Assess whether the implementation specification is a reasonable and appropriate safeguard in the Practice’s environment when analyzed in connection with reference to the likely contribution of protecting the Practice’s electronic PHI,<sup>16</sup> and
- As applicable to the Practice
  - (a) implement the specification if reasonable and appropriate, or
  - (b) if implementation of the specification is not reasonable and appropriate:
    - (i) document the reasons for such a conclusion and
    - (ii) implement an equivalent alternative measure if reasonable and appropriate.<sup>17</sup>

The Practice must consider several factors, including but not limited to, risk analysis, risk mitigation strategy, existing security measures, and cost of implementation.<sup>18</sup> Therefore, each addressable specification must be closely examined and sufficient documentation must be prepared and maintained to demonstrate the basis for the decision and alternative meas-

*Continued on page 10*

Continued from page 9

ures taken, if any. The key in this regard is to document good faith efforts to comply with the HIPAA Security Regulations.

The general requirements imposed upon the Practice under the HIPAA Security Regulations include the following:

- Ensure the confidentiality, integrity and availability of all electronic PHI that the Practice creates, receives, maintains or transmits,<sup>19</sup>
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such electronic PHI,<sup>20</sup>
- Protect against any reasonably anticipated uses or disclosures of such electronic PHI that are not permitted or required under the HIPAA Security Regulations,<sup>21</sup> and
- Ensure compliance with the HIPAA Security Regulations by its workforce.<sup>22</sup>

DHHS noted that it received numerous comments to the proposed HIPAA Security Regulations. The comments confirmed the basic assumption that covered entities affected by the final regulations are varied in size, installed technology, resources, and relative risk.<sup>23</sup> As such, it is impossible to establish a specific set of requirements that could be used by all covered entities.<sup>24</sup> Therefore, DHHS, in the adoption of the final HIPAA Security Regulations, permits greater flexibility in implementation of the final regulations than initially permitted in the proposed regulations.<sup>25</sup> As such, the Practice may use any security measures that allow it to reason-

ably and appropriately implement the standards and implementation specifications in the HIPAA Security Regulations.<sup>26</sup> While evaluating the exact security measures to implement, the Practice must take into account the following:

- the Practice's size, complexity, and capabilities,
- the Practice's technical infrastructure, hardware, and software security capabilities,
- the cost of security measures, and
- the probability and criticality of potential risks to electronic PHI.<sup>27</sup>

Finally, the Practice is required to review and modify, as needed, the measures taken to comply with the HIPAA Security Regulations in order to continue providing reasonable and appropriate protection of electronic PHI.<sup>28</sup>

The HIPAA Security Regulations require the Practice to implement two general standards regarding its practices and procedures:

1. *Policies and procedures.* The Practice must implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Regulations. The Practice may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the HIPAA Security Regulations.<sup>29</sup>

2. *Documentation.*

- The Practice is required to maintain the policies and procedures implemented to comply with the HIPAA

Security Regulations in written or electronic form,<sup>30</sup> and

- If an action, activity, or assessment is required by the HIPAA Security Regulations to be documented, the Practice must maintain a written or electronic record of such action, activity, or assessment.<sup>31</sup> This standard has three required implementation specifications:

(a) *Time limit.* The Practice must retain such documentation for at least six (6) years from the date of its creation or the date when it last was in effect, whichever is later.<sup>32</sup>

(b) *Availability.* The Practice must make such documentation available to those persons responsible for implementing the procedures to which the documentation pertains.<sup>33</sup>

(c) *Updates.* The Practice must periodically review such documentation, and update as needed, in response to environmental or operational changes affecting the security of the electronic PHI.<sup>34</sup>

#### A. *Administrative Safeguards*

The first broad category under the HIPAA Security Regulations is the implementation of administrative safeguards.<sup>35</sup> Administrative safeguards are defined as administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of a covered entity's workforce in relation to the protection of such information.<sup>36</sup> The administrative safeguards can be broken down into the following nine standards:

1. Security management process
2. Assigned security responsibility
3. Workforce security
4. Information access management
5. Security awareness and training
6. Security incident procedures
7. Contingency plan
8. Evaluation
9. Business associate contracts and other arrangements

These standards and the relevant implementation specifications are discussed below.

#### 1. *Security management process.*

The Practice is required to implement policies and procedures to prevent, detect, contain, and correct security violations.<sup>37</sup> This standard is the starting point for the Practice's initial and ongoing efforts to comply with the HIPAA Security Regulations. As technology is continually evolving, so must the Practice's policies and procedures be continuously reviewed and revised to address past experiences and future risks. This standard contains four required implementation specifications.

- (a) *Risk analysis.* The Practice is required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its electronic PHI.<sup>38</sup> The Practice may find it helpful to consider several factors

when conducting such an assessment. The Practice should conduct a thorough review of its technologies and document all of its efforts to assess the risks and vulnerabilities to electronic PHI, and should document all meetings, discussions, etc., taken to make this assessment. The Practice should also focus its efforts towards eliminating or reducing threats to the security of its electronic PHI in the order of severity of the risks.

Perhaps one of the greatest threats to the security of electronic PHI will likely come from past and present workforce members and may be due to intentional or unintentional conduct. Past and present members may have the greatest access to the Practice's electronic PHI and may be able to do the greatest amount of damage very quickly. The Practice should evaluate such risks and tailor its compliance efforts accordingly. After past and present workforce members, vendors such as software consultants, billing companies, etc., will likely have the next greatest access to the Practice's electronic PHI. Next, persons and entities with no direct connection to the Practice, such as computer hackers, must be considered. Also, the Practice should also consider other threats to the security of electronic PHI such as natural disasters and risk of war and/or terrorism.

DHHS notes that a thorough and accurate risk analysis would consider all

of the relevant losses that would be expected if security measures were not in place.<sup>39</sup> Such relevant losses include those caused by unauthorized uses and disclosures of electronic PHI and the loss of data integrity that would be expected to occur if the HIPAA Security Regulations' requirements were not implemented.<sup>40</sup>

In its comments, DHHS references the National Institute of Standards and Technology (NIST) Special Publication (SP) 80030 (NIST SP 800-30).<sup>41</sup> This publication includes a chapter on Risk Assessment and a chapter on Risk Mitigation. NIST SP 800-30 sets forth a nine-step risk assessment methodology.<sup>42</sup> The Practice is encouraged to review this publication as part of its risk analysis.<sup>43</sup>

(b) *Risk management.* The Practice is required to implement security measures that are sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level.<sup>44</sup>

(c) *Sanction policy.* The Practice is required to apply appropriate sanctions against its workforce members who fail to comply with the its security policies and procedures.<sup>45</sup> For consistency and clarity, such policies and procedures should be consistent with the Practice's sanctions adopted pursuant to the HIPAA Privacy Regulations.

(d) *Information system activity review.* The Practice is required to implement procedures to regularly review

records of information system activity such as audit logs, access reports, and security incident tracking reports.<sup>46</sup> DHHS notes that the purpose for this requirement is to promote the periodic review of internal security controls.<sup>47</sup> The extent, frequency, and nature of such reviews should be determined by the Practice's security environment.<sup>48</sup>

2. *Assigned Security Responsibility.* Although the Practice is required to identify a security official (Security Officer) responsible for the development and implementation of policies and procedures required by the HIPAA Security Regulations,<sup>49</sup> there are no implementation specifications established to use as a standard. If the Security Officer is also be the Privacy Officer appointed pursuant to the HIPAA Privacy Regulations, the Practice might consider requiring the Security Officer report to the Privacy Officer to facilitate consistency in the Practice's application of its policies and procedures.

3. *Workforce Security.* The Practice is required to implement policies and procedures to ensure that its workforce members have appropriate access to electronic PHI and to prevent workforce members who do not have access from obtaining the right to use electronic PHI.<sup>50</sup> This standard has three addressable implementation specifications:

(a) *Authorization and/or supervision.* If implemented, this specification would require the Practice to employ procedures for the authorization and/or supervision of workforce members who work

with electronic PHI and locations where it might be accessed.<sup>51</sup> The Practice must consider the appropriate supervision and/or authorization level for every point of access to electronic PHI for the Practice. On-site and off-site locations must also be considered.

The size of the Practice will significantly influence whether the Practice implements this specification. For example, a Practice with only one physician whose staff only consists of the physician's spouse may not need to implement this specification.<sup>52</sup>

(b) *Workforce clearance procedure.* This specification, if implemented, would require the Practice to employ procedures to ensure that a workforce member's access to electronic PHI is appropriate.<sup>53</sup> The need and the extent of the Practice's screening process for members of its workforce should be based on an evaluation of the risk, cost, benefit, feasibility, and other protective measures that exist.<sup>54</sup> Further, the size of the Practice is a relevant consideration. For example, a formal clearance procedure would likely not be reasonable or appropriate for a Practice consisting of a single physician whose only workforce member is the physicians' spouse.<sup>55</sup>

(c) *Termination procedures.* This specification, if implemented, would require the Practice to employ procedures for terminating access to electronic PHI.<sup>56</sup> As discussed above, former workforce members present one

*Continued on page 12*

of the greatest threats to the security of the Practice's PHI. As such, the Practice should carefully consider implementing this specification and considering all of the required actions that must be taken by the Practice including, but not limited to, changing computer password(s) of the entire staff and changing physical locks to the offices.

**4. Information access management.** The Practice must implement policies and procedures to authorize access to electronic PHI consistent with the HIPAA Privacy Regulations.<sup>57</sup> The two addressable implementation specifications that apply to the Practice include the following:<sup>58</sup>

*(a) Access authorization.* This specification, if implemented, would require the Practice to employ policies and procedures for granting access to electronic PHI through, for example, access to a workstation, transaction, program, process, or other mechanism.<sup>59</sup> Consideration should be given to conducting credit and criminal background checks before granting permission to an employee to access electronic PHI.

This implementation specification is sensitive to the size of the Practice. For example, a single physician Practice with a staff of one person may determine that it is unreasonable and inappropriate to implement this specification.

*(b) Access establishment and modification.* This specifica-

tion, if implemented, would require the Practice to employ policies and procedures that, based upon the Practice's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.<sup>60</sup>

**5. Security awareness and training.** The Practice is required to implement a security awareness and training program for its workforce members.<sup>61</sup> Such training applies to all of the Practice's workforce members, including management. Further, such training must be reasonable and appropriate to each member of the workforce necessary to enable each member to complete his other functions for the Practice.<sup>62</sup> Please note that every person who has access to the Practice's electronic PHI must be advised as to the appropriate security measures to reduce improper access, uses, and disclosures.<sup>63</sup> Even persons with access of limited duration, for example, only one day, must be trained.<sup>64</sup> However, such training should be tailored as appropriate. Further, training is not limited to a single occurrence such as an orientation program, but is intended as an ongoing, ever-evolving process.<sup>65</sup> Please note that while training is required to be provided to the Practice's workforce, there is no requirement that training be provided to any of the Practice's business associates.<sup>66</sup>

In its comments, DHHS also recommends NIST SP 800-16, *Information Technology Security Training Requirements, A role and performance base model*, April 1998, as an "excellent

source of information and guidance on this subject."<sup>67</sup>

*(a) Security reminders.* This specification, if implemented, would require the Practice to provide periodic security updates.<sup>68</sup> The Practice should consider incorporating such updates with general privacy reminders as part of its ongoing compliance with the HIPAA Privacy Regulations.

*(b) Protection from malicious software.* This specification, if implemented, would require the Practice to adopt procedures for guarding against, detecting, and reporting malicious software.<sup>69</sup> Due to the relatively low cost for software to protect against viruses, it may be unreasonable for the Practice to not implement this specification, at least in part.

*(c) Log-in monitoring.* This specification, if implemented, would require the Practice to employ procedures for monitoring log-in attempts and reporting discrepancies.<sup>70</sup>

*(d) Password management.* This specification, if implemented, would require the Practice to employ procedures for creating, changing, and safeguarding passwords.<sup>71</sup> The Practice should consider changing passwords at least monthly. In addition, the Practice should ensure that all passwords are "alphanumeric," i.e., contain both letters and numbers to make "cracking" the passwords more difficult.

**6. Security incident procedures.** The Practice is required to implement policies and procedures to address security inci-

dents.<sup>72</sup> This standard has one required implementation specification:

*Response and Reporting.* The Practice must:

- identify and respond to suspected or known security incidents,
- mitigate, to the extent practicable, harmful effects of security incidents that are known to the Practice, and
- document security incidents and outcomes.<sup>73</sup>

DHHS recognizes that this specification is an integral component of a security program.<sup>74</sup> Please note that this specification does not require that the Practice report any incidents to any governmental agencies, including DHHS.<sup>75</sup> However, the Practice may want to consult with legal counsel to determine when such reporting to a governmental entity may be necessary.

**7. Contingency plan.** The Practice is required to establish, and implement as needed, policies and procedures for responding to emergencies or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that damage systems containing electronic PHI.<sup>76</sup> This standard has the following implementation specifications:

*(a) Data backup plan.* The Practice is required to establish and implement procedures to create and maintain retrievable exact copies of electronic PHI.<sup>77</sup> Such procedures may involve daily backup of electronic PHI to a secure off-site location.

*(b) Disaster recovery plan.* The Practice is required to estab-

lish, and implement as needed, procedures to restore any loss of data.<sup>78</sup> DHHS notes that recent events, including those that occurred on September 11, 2001, demonstrate the significance of such planning.<sup>79</sup> Further, DHHS considers this specification to be a reasonable precaution.<sup>80</sup>

(c) *Emergency mode operation plan.* The Practice is required to establish, and implement as needed, procedures to enable the continuation of its critical business processes for protection of the security of electronic PHI while operating in emergency mode.<sup>81</sup>

(d) *Testing and revision procedures.* This specification, if implemented, would require the Practice to employ procedures for periodic testing and revision of its contingency plans.<sup>82</sup> The Practice may consider coordinating such testing to correspond with tests of its privacy practices.

(e) *Applications and data criticality analysis.* This specification, if implemented, would require the Practice to assess the relative criticality of specific applications and data in support of other contingency plan components.<sup>83</sup>

8. *Evaluation.* The Practice is required to perform a periodic technical and nontechnical evaluation that establishes the extent to which the Practice's security policies and procedures meet the requirements of the HIPAA Security Regulations.<sup>84</sup> Such evaluation should initially be based upon the standards implemented under

the HIPAA Security Regulations and, subsequently, would be in response to environmental or operational changes that affect the security of the Practice's electronic PHI.

9. *Business associate contracts and other arrangements.* The Practice may permit a "business associate" to create, receive, maintain, or transmit electronic PHI on behalf of the Practice, only if the Practice obtains satisfactory assurances that the business associate will appropriately safeguard such information.<sup>85</sup> A business associate is defined as a person who:

(a) On behalf of a covered entity, other than in the capacity of a member of the workforce of such covered entity, performs, or assists in the performance of:

- a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing,
- any other function or activity regulated by the HIPAA Privacy Regulations, or

(b) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized healthcare

arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.<sup>86</sup>

This standard has one required implementation specification.

*Written contract or other arrangement.* The Practice is required to have a written contract or other arrangement with the business associate that meets at a minimum, four requirements. The business associate must agree to:

- implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the Practice,<sup>87</sup>
- ensure that any agent, including a subcontractor, to whom it provides such electronic PHI agrees to implement reasonable and appropriate safeguards to protect it,<sup>88</sup>
- report to the Practice any security incident of which it becomes aware,<sup>89</sup> and
- authorize termination of the contract by the Practice, if the Practice determines that the business associate has violated a material term of the contract.<sup>90</sup>

## B. Physical Safeguards

The second broad category under the HIPAA Security Regulations is the implementation of physical safeguards. Physical safeguards are defined as physical measures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.<sup>91</sup> Such safeguards go beyond the security of electronic PHI and extend to the Practice's facility, which includes the physical premises and the interior and exterior of a building.<sup>92</sup> As can be understood by reviewing the specific standards and relevant specifications, implementation is highly fact sensitive and must be tailored to the Practice's facility. The physical safeguards can be broken down into the following four standards:

1. Facility access controls
2. Workstation use
3. Workstation security
4. Device and media controls

1. *Facility access controls.* The Practice is required to implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which systems are contained, while also ensuring that properly authorized access is allowed.<sup>93</sup> The implementation specifications for this standard are all addressable and are set forth below:

(a) *Contingency operations.* This specification, if implemented, would require the Practice to establish (and employ as needed) procedures that

*Continued on page 14*

allow facility access in order to restore lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.<sup>94</sup>

(b) Facility security plan. This specification, if implemented, would require the Practice to employ policies and procedures to safeguard its facility and equipment from unauthorized physical access, tampering, and theft.<sup>95</sup> If the Practice shares space in a building, the impact of other person's and/or entity's security plan should be considered.<sup>96</sup>

(c) Access control and validation procedures. This specification, if implemented, would require the Practice to employ procedures to control and validate a person's access to its facility based on the person's role or function.<sup>97</sup> This specification includes visitor control and control of access to software programs for testing and revision.<sup>98</sup>

(d) Maintenance records. This specification, if implemented, would require the Practice to employ policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).<sup>99</sup>

2. *Workstation Use.* The Practice must implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific worksta-

tion or class of workstation that can access electronic PHI.<sup>100</sup> A workstation is defined as an electronic computing device (for example, a laptop or desktop computer) or any other device that performs similar functions, and electronic media stored in its immediate environment.<sup>101</sup> Therefore, workstations that are used outside of the Practice's facility must also be considered when addressing this standard.

3. *Workstation Security.* The Practice is required to implement physical safeguards for all workstations that access electronic PHI in order to restrict access to authorized users.<sup>102</sup> The appropriate safeguards will depend upon the Practice's risk analysis and risk management programs.<sup>103</sup>

4. *Device and media controls.* The Practice must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI in and out of a facility, and the movement of such items within the Practice's facility.<sup>104</sup>

(a) *Disposal.* The Practice must implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which electronic PHI is stored.<sup>105</sup> Merely deleting electronic PHI is usually not sufficient to ensure that all electronic PHI is removed.

(b) *Media re-use.* The Practice is required to implement procedures for removal of electronic PHI from electronic media before such is made available for re-use.<sup>106</sup>

(c) *Accountability.* This specification, if implemented, would

require the Practice to maintain a record of the movements of hardware and electronic media and any person responsible for the same.<sup>107</sup>

(d) *Data backup and storage.* This specification, if implemented, would require the Practice to create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.<sup>108</sup> The exact data that the Practice needs to backup and the operations necessary to facilitate such backup should be determined by the Practice's risk analysis and risk management processes.<sup>109</sup> However, the information that should be preserved as part of the backup process should be sufficient to enable the Practice to continue operating business "as usual" despite the occurrence of an event that causes loss or destruction of information.<sup>110</sup>

### C. Technical Safeguards

The third broad category under the HIPAA Security Regulations is the implementation of technical safeguards. Technical safeguards are defined as the technology and policies and procedures for the use of technology that protects electronic PHI and controls access to electronic PHI.<sup>111</sup> Such safeguards consist of the following five standards:

1. Access control
2. Audit controls
3. Integrity
4. Person or entity authentication
5. Transmission security

1. *Access control.* The Practice is required to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights.<sup>112</sup>

(a) *Unique user identification.* The Practice is required to assign a unique name and/or number for identifying and tracking user identity.<sup>113</sup>

(b) *Emergency access procedure.* The Practice is required to establish, and implement as needed, procedures for obtaining necessary electronic PHI during an emergency.<sup>114</sup>

(c) *Automatic logoff.* This specification, if implemented, would require the Practice to employ electronic procedures that terminate an electronic session after a predetermined time of inactivity.<sup>115</sup>

(d) *Encryption and decryption.* This specification, if implemented, would require the Practice to employ a mechanism to encrypt and decrypt electronic PHI.<sup>116</sup>

2. *Audit controls.* The Practice is required to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems<sup>117</sup> that contain or use electronic PHI.<sup>118</sup> DHHS notes NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems* and NIST SP 800-33 *Underlying Technical Models for Information Technology Security* as potential references in implementing this standard.<sup>119</sup>

3. *Integrity.* The Practice is required to implement policies

and procedures to protect electronic PHI from improper alteration or destruction.<sup>120</sup> This standard has only one implementation specification that is addressable.

(a) *Mechanism to authenticate electronic PHI.* This specification, if implemented, would require the Practice to employ electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.<sup>121</sup>

4. *Person or entity authentication.* The Practice is required to implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.<sup>122</sup>

5. *Transmission security.* The Practice is required to implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.<sup>123</sup>

(a) *Integrity controls.* This addressable implementation specification, if implemented, would require the Practice to employ security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.<sup>124</sup>

(b) *Encryption.* This specification, if implemented, would require the Practice to implement a mechanism to encrypt electronic PHI whenever deemed appropriate.<sup>125</sup>

In conducting an assessment of the Practice, do not focus entirely on its technology. The first review should be made of

administrative issues that do not require changing current technology. Further, determine what technology is needed based on the Practice's needs. Resist the urge to expend unreasonable amounts on technology that is not appropriate. If you are using a consultant, do not become "victimized" by unnecessary fears that force you to acquire technology that you either do not need or want for the Practice. It is my sincere hope that Practices reviewing this article will better understand their obligations under the HIPAA Security Regulations.

Finally, make sure that all of your efforts to comply with the HIPAA Security Regulations are reflected in your HIPAA Privacy Policies and Procedures Manual.

### III. Conclusion

DHHS has noted in the commentary to the adoption of the HIPAA Security Regulations that it plans to issue guidance documents in the future. A Practice is encouraged to periodically check the DHHS website at [www.aspe.hhs.gov/admnsimp](http://www.aspe.hhs.gov/admnsimp) in order to obtain a copy of such guidance materials as soon as it is listed.

Please note that in the comments to the HIPAA Security Regulations, DHHS points out that a number of voluntary national and regional organizations have been formed to address implementation issues under various HIPAA regulations.<sup>126</sup> One such organization is the Workgroup for Electronic Data Interchange (WEDI).<sup>127</sup> WEDI was named in the HIPAA statute as an organization that would consult with the Secretary of DHHS regarding

HIPAA issues.<sup>128</sup> DHHS also notes that the Strategic National Implementation Process (SNIP) was developed under the auspices of WEDI.<sup>129</sup> Such organizations, including WEDI, have developed white papers, tools, and best practices for addressing various HIPAA standards, including privacy and security standards,<sup>130</sup> and some of these products may be useful in implementing the HIPAA Security Regulations standards.<sup>131</sup> A partial list of such products can be found at [www.wedi.org/snip](http://www.wedi.org/snip). DHHS notes that while such products may provide valuable assistance in implementing the security standards, it did not endorse any such products and that the user must determine the appropriateness of such products.<sup>132</sup>

While the effective date for the HIPAA Security Regulations is April 20, 2005, the Practice should begin the process of implementing the requirements now. As discussed above, it will take at least one year to properly implement the HIPAA Security Regulations. In addition, under the HIPAA Privacy Regulations "mini-Security Rule," many of the HIPAA Security Regulations would be appropriate to implement immediately.

### Endnotes

<sup>1</sup> Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).

<sup>2</sup> Covered entities are defined as (1) health plans, (2) health care clearinghouses, and (3) health care providers who transmit any health information in electronic form in connection with a covered transaction. 45 C.F.R. § 164.103 (2003).

<sup>3</sup> Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*

<sup>6</sup> The HIPAA Security Regulations will become effective on April 20, 2005, for all covered entities except for small health plans that have until April 20, 2006, to comply.

<sup>7</sup> The HIPAA Privacy Regulations became effective April 14, 2003, for covered entities except for small health plans that have until April 14, 2004, to comply.

<sup>8</sup> 45 C.F.R. 164.530(c)(1).

<sup>9</sup> 45 C.F.R. § 164.302 (2003).

<sup>10</sup> 45 C.F.R. § 164.103 (2003)

<sup>11</sup> *Id.*

<sup>12</sup> See 45 C.F.R. § 164.306 (2003).

<sup>13</sup> The exceptions set forth under the HIPAA Privacy Regulations for PHI are as follows: education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C.A. 1232g, those records described at 20 U.S.C.A. § 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as an employer 45 C.F.R. 160.103. There is also an exception for PHI that has been re-identified in accordance with 45 C.F.R. § 164.514.

<sup>14</sup> 68 C.F.R. § 342 (2003).

<sup>15</sup> Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8342 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).

<sup>16</sup> 45 C.F.R. § 164.306(d)(3)(i).

<sup>17</sup> 45 C.F.R. § 164.306(d)(3)(ii)(A)-(B).

<sup>18</sup> Health Insurance Reform: Security Standards, 68 Fed. Reg.

|  |  |   |  |
|--|--|---|--|
| <p><i>Continued from page 15</i></p> <p>8334, 8336 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>19 45 C.F.R. § 164.306(a)(1).</p> <p>20 45 C.F.R. § 164.306(a)(2).</p> <p>21 45 C.F.R. § 164.306(a)(3).</p> <p>22 45 C.F.R. § 164.306(a)(4); Workforce is defined as employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Practice, is under the direct control of such entity, whether or not they are paid by the Practice. 45 C.F.R. § 160.103 (2003).</p> <p>23 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>24 <i>Id.</i></p> <p>25 45 C.F.R. § 164.306(b).</p> <p>26 45 C.F.R. § 164.306(b)(1).</p> <p>27 45 C.F.R. § 164.306(b)(2).</p> <p>28 45 C.F.R. § 164.306(e).</p> <p>29 45 C.F.R. § 164.316(a).</p> <p>30 45 C.F.R. § 164.316(b)(1)(i).</p> <p>31 45 C.F.R. § 164.316(b)(1)(ii).</p> <p>32 45 C.F.R. § 164.316(b)(2)(i).</p> <p>33 45 C.F.R. § 164.316(b)(2)(ii).</p> <p>34 45 C.F.R. § 164.316(b)(2)(iii).</p> <p>35 45 C.F.R. § 164.308 (2003).</p> <p>36 45 C.F.R. § 164.304 (2003).</p> <p>37 45 C.F.R. § 164.308(a)(1)(i).</p> <p>38 45 C.F.R. § 164.308(a)(1)(ii)(A).</p> <p>39 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8347 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>40 <i>Id.</i></p> | <p>41 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8346 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>42 NIST SP 800-30, page 8.</p> <p>43 NIST SP 800-30. Other important NIST publications can be obtained at <a href="http://www.csrc.nist.gov/publications/nistpubs/index.html">www.csrc.nist.gov/publications/nistpubs/index.html</a>.</p> <p>44 45 C.F.R. § 164.308(a)(1)(ii)(B).</p> <p>45 45 C.F.R. § 164.308(a)(1)(ii)(C).</p> <p>46 45 C.F.R. § 164.308(a)(1)(ii)(D).</p> <p>47 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8347 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>48 <i>Id.</i></p> <p>49 45 C.F.R. § 164.308(a)(2).</p> <p>50 45 C.F.R. § 164.308(a)(3)(i).</p> <p>51 45 C.F.R. § 164.308(a)(3)(ii)(A).</p> <p>52 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8347 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>53 45 C.F.R. § 164.308(a)(3)(ii)(B).</p> <p>54 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8348 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>55 <i>Id.</i></p> <p>56 45 C.F.R. § 164.308(a)(3)(ii)(C).</p> <p>57 45 C.F.R. § 164.308(a)(4)(i).</p> <p>58 The HIPAA Security Regulations also include a third implementation specification that applies to health care clearing houses, providing that if a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic PHI of the clearinghouse from unauthorized access by the larger organization. 45 C.F.R. §</p> | <p>164.308(a)(4)(ii)(A).</p> <p>59 45 C.F.R. § 164.308(a)(4)(ii)(B).</p> <p>60 45 C.F.R. § 164.308(a)(4)(ii)(C).</p> <p>61 45 C.F.R. § 164.308(a)(5)(i).</p> <p>62 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8349 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>63 <i>Id.</i></p> <p>64 <i>Id.</i></p> <p>65 <i>Id.</i></p> <p>66 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8350 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>67 <i>Id.</i></p> <p>68 45 C.F.R. § 164.308(a)(5)(ii)(A).</p> <p>69 45 C.F.R. § 164.308(a)(5)(ii)(B).</p> <p>70 45 C.F.R. § 164.308(a)(5)(ii)(C).</p> <p>71 45 C.F.R. § 164.308(a)(5)(ii)(D).</p> <p>72 45 C.F.R. § 164.308(a)(6)(i).</p> <p>73 45 C.F.R. § 164.308(a)(6)(ii).</p> <p>74 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8350 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>75 <i>Id.</i></p> <p>76 45 C.F.R. § 164.308(a)(7)(i).</p> <p>77 45 C.F.R. § 164.308(a)(7)(ii)(A).</p> <p>78 45 C.F.R. § 164.308(a)(7)(ii)(B).</p> <p>79 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8351 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>80 <i>Id.</i></p> <p>81 45 C.F.R. § 164.308(a)(7)(ii)(C).</p> <p>82 45 C.F.R. § 164.308(a)(7)(ii)(D).</p> | <p>83 45 C.F.R. § 164.308(a)(7)(ii)(E).</p> <p>84 45 C.F.R. § 164.308(a)(8).</p> <p>85 45 C.F.R. § 164.308(b)(1); This standard does not apply to the Practice's transmission of electronic PHI to a health care provider concerning treatment for an individual. 45 C.F.R. § 164.308(b)(2)(i).</p> <p>86 45 C.F.R. § 160.103 (2003).</p> <p>87 45 C.F.R. § 164.314(a)(2)(A).</p> <p>88 45 C.F.R. § 164.314(a)(2)(B).</p> <p>89 45 C.F.R. § 164.314(a)(2)(C).</p> <p>90 45 C.F.R. § 164.314(a)(2)(D); The HIPAA Security Regulations provide certain exceptions if the Practice and its business associate are governmental entities. 45 C.F.R. § 164.308(b).</p> <p>91 45 C.F.R. § 164.304 (2003).</p> <p>92 <i>Id.</i></p> <p>93 45 C.F.R. § 164.310(a)(1).</p> <p>94 45 C.F.R. § 164.310(a)(2)(i).</p> <p>95 45 C.F.R. § 164.310(a)(2)(ii).</p> <p>96 <i>See</i> Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8353 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>97 45 C.F.R. § 164.310(a)(2)(iii).</p> <p>98 <i>Id.</i></p> <p>99 45 C.F.R. § 164.310(a)(2)(iv).</p> <p>100 45 C.F.R. § 164.310(b).</p> <p>101 45 C.F.R. § 164.304 (2003).</p> <p>102 45 C.F.R. § 164.310(c).</p> <p>103 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8354 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).</p> <p>104 45 C.F.R. § 164.310(d)(1).</p> <p>105 45 C.F.R. § 164.310(d)(2)(i).</p> |
|--|--|---|--|

- 106 45 C.F.R. § 164.310(d)(2)(ii).
- 107 45 C.F.R. § 164.310(d)(2)(iii).
- 108 45 C.F.R. § 164.310(d)(2)(iv).
- 109 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8354 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).
- 110 *Id.*
- 111 45 C.F.R. § 164.304 (2003).
- 112 45 C.F.R. § 164.312(a)(1).
- 113 45 C.F.R. § 164.312(a)(2)(i).
- 114 45 C.F.R. § 164.312(a)(2)(ii).
- 115 45 C.F.R. § 164.312(a)(2)(iii).
- 116 45 C.F.R. § 164.312(a)(2)(iv).
- 117 Information systems is defined as an interconnected set of information resources under the same direct management controls that share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. 45 C.F.R. § 164.304 (2003).
- 118 45 C.F.R. § 164.312(b).
- 119 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8355 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164); NIST Publications can be obtained at [www.csrc.nist.gov/publications/nist-pubs/index.html](http://www.csrc.nist.gov/publications/nist-pubs/index.html).
- 120 45 C.F.R. § 164.312(c)(1).
- 121 45 C.F.R. § 164.312(c)(2).
- 122 45 C.F.R. § 164.312(d).
- 123 45 C.F.R. § 164.312(e)(1).
- 124 45 C.F.R. § 164.312(e)(2)(i).
- 125 45 C.F.R. § 164.312(e)(2)(ii); Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential

- process or key. 45 C.F.R. § 164.304 (2003).
- 126 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8336-7 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).
- 127 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8337 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).
- 128 *Id.*
- 129 *Id.*
- 130 *Id.*
- 131 *Id.*
- 132 Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8337 (Feb. 20, 2003) (to be codified at 45 C.F.R. pt. 164).

## Plan to Attend

### Physicians and Physician Organizations Law Institute

February 11-12, 2004

Westin Diplomat Resort & Spa Hollywood, Florida

#### Registration Fees:

- \$695 - AHLA Member
- \$620 - AHLA Member Group Registration Rate
- \$870 - Nonmember

### Hospitals and Health Systems Law Institute

February 12-13, 2004

#### Registration Fees (when registering for both programs):

- \$1120 - AHLA Member
- \$1040 - AHLA Member Group Registration Rate
- \$1290 - Nonmember

### Plan to attend the Practice Group Luncheons Wednesday, February 11

**Physician Organizations** - An open forum discussion on issues of interest to the members of the Physician Organizations Practice Group. Topics to be discussed include:

- Physicians' experiences withdrawing from Medicare
- How malpractice concerns are affecting the scope of physicians' practice. Is it leading to greater specialization, less or neither?
- Are restrictive covenants requiring resignation of hospital privileges enforceable?
- Physician Recruitment by Hospitals and Hospital Systems
- Physician/Hospital Joint Ventures

**Moderators:** Michael Schaff, Wilentz Goldman & Spitzer PA, Woodbridge, NJ, Charlene McGinty, Powell Goldstein Frazer & Murphy LLP, Atlanta, GA, and Lisa Taylor, St. John & Wayne LLC, Newark, NJ

### Thursday, February 12

**Credentialing and Peer Review** - The Hospital Medical Staff Office: How It Operates and What It Needs from Counsel

**Presenter:** Beckie Watson, BSH, CMSC, CPCS, Regulatory Coordinator, St. Vincent's Medical Center, Jacksonville, Florida

**Labor and Employment** - Non-Compete Agreements

- How employers can most effectively enforce non-compete and non-solicitation agreements with their employees;
- How employers can most effectively protect their trade secrets, confidential information and other competitive intelligence.
- The enforceability of non-compete and no solicitation agreements for professionals in the healthcare industry.

**Presenter:** Robert M. Linn, Esquire, Litigation Department Chair, Cohen & Grigsby, Pittsburgh, PA

## Building A “High Performance” Messenger Modeling Engine for Physician Practices

Barney Hebert, JD  
Eron Reid, CPA  
Horne CPA Group  
Hattiesburg, Mississippi

When it comes to reimbursing healthcare providers for their services, insurance companies have long held the advantage. Standing alone, each provider clinic, whether large or small, has little if any leverage to negotiate higher reimbursement from the insurance company. In the early 1990s, some believed that by joining forces into a single network, e.g., an Independent Physicians Association (IPA) or Physician-Hospital Organization (PHO), providers could create sufficient leverage that would lead to stronger, more effective negotiating power. Time showed, however, that while such joined forces could deliver greater efficiencies and financial savings, the tables could not be so easily turned in terms of the core reimbursement challenges. Today, a stronger case can be made for a different vehicle—a properly constructed messenger model—as the key to shifting reimbursement into high (and more effective) gear.

### I. Understanding the Model

While many providers believe that the main purpose of a messenger model organization is to negotiate higher reimbursement with managed care organizations, the fact is anti-trust regulations prohibit these organizations from collectively setting

fees in the marketplace. When designed and used properly, however, messenger model provider organizations create value for their members by providing a wealth of information concerning managed care contracting; information that, in turn, leads to the improvement in negotiating power that was originally sought.

By consistently receiving information concerning fees, contract terms, and payer profiles, members are able to make more informed decisions such as whether to participate in discounted fee-for-service contracts. Physicians armed with the appropriate data are also more likely to be successful in negotiating contracts that offer higher reimbursement rates by payers. If correctly created, the messenger model serves as an analytical tool which each network provider can use independently from his/her/their competitors to make a more informed decision whether to opt-in or opt-out of a potential discounted fee-for-service contract offer. Simply stated, properly constructed messenger model engines assist provider organizations in winning the race against payers.

### II. Pros and Cons of Format Alternatives

Creating a messenger model includes deciding the format in which fee information will be messaged to providers. IPA and PHO members must supply the messenger with minimum fees they are willing to accept from payers. The most common methods for messaging minimum reimbursement amounts are the following: for the members to determine and convey their minimum fees for their top

20 CPT codes; for them to convey their minimum Medicare multiples by CPT code sub-section; or for them to convey their minimum block conversion factors based on Ingenix RVUs by CPT code sub-section. The advantages and disadvantages of each method are as follows:

#### A. Minimum Fees for Top 20 CPT Codes

*Advantage:* Physicians are very familiar with their highest revenue producing codes and often request reimbursement information for these codes from payers. For the majority of specialties, the top 20 producing CPT codes account for approximately 80% of the physician’s revenues. Therefore, this is a very straightforward model. The messenger simply forwards the payers proposed allowables for the top 20 CPT codes as compared to the minimum fees provided by the physician.

*Disadvantage:* The messenger model becomes difficult to maintain. Depending on the size of the provider organization the database of top CPT codes may be in excess of 1,000 codes. Certain specialties such as radiology have to provide in excess of 100 CPT codes in order to capture at least 80% of their revenues. Often times, the majority of contracts have to be messaged to the entire network due to a handful of CPT codes in which the payers’ offer is below the physician’s minimum fee.

#### B. Minimum Medicare Multiples by CPT Code Sub-Section

*Advantage:* Physicians are accustomed to benchmarking their fees using the Medicare fee schedule. The physician simply provides the messenger with the

minimum Medicare multiple they are willing to accept from payers for each applicable CPT code sub-section. In recent years, several payers have aligned their fee schedule with Medicare, basing their reimbursement on a percentage of the Medicare fee schedule. Therefore, this methodology potentially increases the efficiency of the messenger to facilitate contracts between the provider organization and payer.

*Disadvantage:* The process of setting the initial minimum percentage is more complicated than just providing a minimum fee. In addition, many physicians do not agree with the methodology that Medicare uses in setting fees and therefore, do not want their minimum reimbursement amounts associated with the Medicare fee schedule. For certain specialties such as pathology and psychology, the minimums based on Medicare are not applicable and carve-outs have to be created.

#### C. Minimum Block Conversion Factors by CPT Code Sub-Section

Certain provider organizations utilize block conversion factors based on Ingenix RVUs in setting minimum fees. For example, the physician may provide a block conversion factor of 6.5 for all codes appearing in the Evaluation and Management CPT code sub-section. In order to determine the physician’s minimum fee for CPT code 99213, you would simply multiply 6.5 by Ingenix’s RVU of 10.0 resulting in a minimum reimbursement amount of \$65.

*Advantage:* Using this methodology is similar to minimums based on Medicare multiples

and it is easier for the messenger to facilitate contracts. In addition, RVUs determined by Ingenix are not influenced by politics and therefore some codes are easier to understand and are considered more reliable by some physicians.

*Disadvantage:* Block conversion factors and Ingenix RVUs are not as well recognized as the Medicare fee schedule. Therefore, whenever implementing this messaging strategy a considerable amount of training on the front-end is required. In addition, some payers have to be educated concerning the use of this methodology.

### III. Conclusion

While there is no one perfect model for messaging physicians minimum reimbursement amounts, the following key points should be considered in choosing a messaging strategy:

- Insure that your messenger model is abiding by the letter of the law and is not allowing physicians to collectively bargain with payers.
- Align your messenger model with your market. For example, if the majority of your physician members have a low Medicare payer mix, then you would not want to implement a model based on Medicare multiples.
- Most importantly, make sure that physicians understand the model and are in agreement with the way in which pricing information is being messaged, and can (or cannot) be messaged, in accordance with applicable law.

## Health Lawyers' Publications

---

### Peer Review Guidebook, 3<sup>rd</sup> Edition

*By AHLA Credentialing and Peer Review (CPR) Practice Group*

This new edition completely updates the case law, reviews the threshold issues, presents analysis of the Health Care Quality Improvement Act (HCQIA), new chapters on injunctive relief from peer-review actions and more!

© 2003, approximately 180 pages, perfect bound, Practice Guide Item Code: WAA200301

Member \$75 / Nonmember \$90

### False Claims Act and The Healthcare Industry: Counseling and Litigation

*By Robert Salcido, Esquire*

This supplement will give you up-to-date FCA developments so you can advise your clients on how to assess their company's exposure to liability, evaluate the exposure of acquired companies, and reform practices to reduce potential FCA liability.

© 2003, 284 pages, perfect bound, Cornerstone Series Supplement

Item Code: WB200302S

Member \$65 / Nonmember \$55

### Indemnification in Healthcare Contracting, 2<sup>nd</sup> Edition

*By Susan O. Scheutzow, Esquire*

Analyzes in depth the nature of indemnity as used in the healthcare industry, the choices to be made when drafting a contract, and the potential implications for the contracting parties' liability to each other and to third parties.

© 2003, 45 pages plus front matter, spiral bound, Expert Series

Item Code: WM200302

Member \$50 / Nonmember \$60

### Lawyers as HIPAA Business Associates

*By Kristen B. Rosati, Esquire, and Edward F. Shay, Esquire*

Analyzes the nature of Business Associate Agreements under the provisions of the Health Insurance Portability and Accountability Act (HIPAA) as it applies to lawyers and their healthcare clients.

© 2003, 45 pages plus front matter, spiral bound, Expert Series

Item Code: WM200303

Member \$55 / Nonmember \$65

To Order: go to [www.healthlawyers.org/ecommerce](http://www.healthlawyers.org/ecommerce) or call the Member Service Center at (202) 833-0766



AMERICAN  
**HEALTH LAWYERS**  
ASSOCIATION

1025 Connecticut Ave, NW, Suite 600  
Washington, DC 20036-5405  
Phone: (202) 833-1100  
Fax: (202) 833-1105  
[www.healthlawyers.org](http://www.healthlawyers.org)

**JOIN Us!**

***Mid-Year Luncheon Meeting***

**Physician Organizations Practice Group**

*Wednesday, February 11, 2004*

**Physicians and Physician Organizations Law Institute**

*February 11-12, 2004 • Westin Diplomat Resort & Spa • Hollywood, Florida*

*More Information on page 17 and to register, go to [www.healthlawyers.org/programs/prog\\_04phys.cfm](http://www.healthlawyers.org/programs/prog_04phys.cfm)*

Winter 2003 Volume 6 Issue 2

**Physician  
Organizations**

