

Radiology Administrator's Compliance & Reimbursement Insider

J U N E 2 0 0 1

IN THIS ISSUE

Set Policy for Secure Use of Portable Computers..... 1

Portable computers pose security risks to your health information. Here's a policy to help you prevent information from being lost or stolen—and help you comply with proposed HIPAA security regs.

► Model Policy: Set Requirements for Appropriate and Secure Use of Portable Computer (pp. 3–4)

In the News: HCFA Expands PET Scan Coverage..... 5

Plugging Loopholes: Make Sure Exclusive Contract with Hospital Is Really Exclusive..... 7

“Exclusive” contracts aren't always what they seem—here are some ways to make sure your exclusive agreement gives your practice the sole right to perform radiology services.

Understanding Corporate Integrity Agreements..... 8

At some point your practice, your hospital, or one of your vendors may be operating under a corporate integrity agreement—a tool the OIG uses to prevent fraud and abuse by those who have had trouble in the past. Here's what you need to know about these agreements.

► Special Risks of a Corporate Integrity Agreement (p. 10)

IN FUTURE ISSUES

- New Stark Regulations Permit Per Use Arrangements
- Follow These Guidelines in Your Medical Director Contracts
- Hidden Risks of Cybermedicine

Set Policy for Secure Use of Portable Computers

You may provide portable computers, such as laptops and notebook computers, to some of your practice's employees (and independent contractors) so they can carry out their duties at the workplace or off site. For instance, coding staff may use portable computers so they can work from home. Or radiologists may carry them around the hospital or take them home to do their reports and other work.

Portable computers can be very convenient and make work more efficient. But they pose risks to the security of your health information. Compared with desktop computers on your network, portable computers are more susceptible to loss or theft, more vulnerable to viruses, and are subject to security breaches that are tough to identify and correct.

To lessen these security risks, set a policy on the use of portable computers, recommends health information attorney Jonathan Tomes. Having such a policy should help prevent health information on a portable computer from being lost or compromised. It also should help your HIPAA compliance efforts—since the proposed HIPAA security regulations require you to have “media controls” that govern the receipt and removal of hardware and software into and out of your organization. We provide you with a Model Policy on pp. 3–4, based on a policy that was written by Tomes. You can adapt it for use in your organization.

What Policy Should Say

Your policy, like our Model Policy, should start with an explanation of the policy's general purpose—protecting the confidentiality of your medical information. It should also require that all employees who use portable computers be familiar with the policy, says Tomes. And it should alert employees to the security risks of using portable computers.

Next, the policy should tell employees the following, says Tomes:

Written authorization required. Let employees know that they can't use portable computers unless they have written authorization to do so. You'll have to designate who may give this written authorization—in our Model Policy it's the compliance officer.

To ensure even greater accountability and careful consideration of the employee's use, you may want to bring the employee's department head into the decision-making process, notes Tomes. To do this, you can require that the employee's use be recommended for authorization by the department head, Tomes says [Policy, par. 1].

Signed agreement required. Next, as a condition for using a portable computer, require the employee to sign an agreement on his or her portable

(continued on p. 2)

BOARD OF ADVISORS

Jeffrey F. Boothe, Esq.Holland & Knight, LLP
Washington, DC**Kathy Boyle**The Boyle Company
Manchester, MA**Maureen E. Brooks**Insource Medical Solutions
Santa Ana, CA**Andrei Costantino**Parente Randolph Orlando
Carey & Associates, LLC
Harrisburg, PA**Judy A. Dye**University Medical Center
Tucson, AZ**William G. Franz Jr.**Radiologix, Inc.
Dallas, TX**Alice G. Gosfield, Esq.**Alice G. Gosfield and
Assocs., PC
Philadelphia, PA**Thomas W. Greeson, Esq.**Reed Smith Hazel &
Thomas, LLP
Falls Church, VA**Karol Handrahan**University of Maryland
Dept. of Radiology
Baltimore, MD**Roberta J. Miller**Medical College of Ohio
Dept. of Radiology
Toledo, OH**Ronald E. Miller**Medical College of
Virginia Hospitals
Richmond, VA**Diane S. Millman, Esq.**Powers Pyles Sutter & Verville
Washington, DC**Melody Mulaik, MSHS, CPC**Coding Strategies, Inc.
Dallas, GA**Claudia A. Murray**Provider Practice Analysis, LLC
Baldwin, MD**Paula Richburg**QuadraMed
Columbia, MO**William A. Sarraile, Esq.**Arent Fox Kintner Plotkin
& Kahn, PLLC
Washington, DC**John R. Steiner, Esq.**The Cleveland Clinic
Foundation
Cleveland, OH**Tobin N. Watt, Esq.**Smith, Helms, Mulliss & Moore
Atlanta, GAEditor: **Jill K. Gormley, Esq.**Executive Editors: **David B. Klein, Esq.,
Nicole R. Lefton, Esq., Janet Ray**Senior Legal Editor: **Susan R. Lipp, Esq.**Senior Editors: **Nancy Asquith, Heather Ogilvie**Copy Chief: **Tamar M. Friedman**Copy Editor: **Graeme McLean**Proofreaders: **Cynthia Gately, Arthur D. Hlavaty**Production Director: **Mary V. Lopez**Senior Production Associate: **Sidney Short**Director of Planning: **Glenn S. Demby, Esq.**New Project Editors: **Michael T. Borruso, Esq.
Karyn Wynn, Esq.**Direct Marketing Director: **Peter Stowe**List Management Director: **Vijay Thakkar**Data Processing Manager: **Rochelle Conti**Director of Operations: **Michael Koplin**Sales Manager: **Joyce Lembo**Customer Service Rep.: **Helena Therezo**Fulfillment Supervisor: **Edgar A. Pinzón**Financial Manager: **Janet Urbina**Office Management Asst.: **Larry Hjalte**Publisher: **George H. Schaeffer, Esq.**Founders: **Andrew O. Shapiro, Esq., John M. Striker, Esq.****Subscriptions:** *Radiology Administrator's Compliance & Reimbursement Insider* (ISSN 1527-2338) is published monthly. Subscription rate: \$355 for 12 monthly issues. Address all correspondence to: Brownstone Publishers, Inc., 149 Fifth Ave., New York, NY 10010-6801. Tel.: 1-800-643-8095 or (212) 473-8200; fax: (212) 473-8786; e-mail: jgormley@brownstone.com**Disclaimer:** This publication provides general coverage of its subject area. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional advice or services. If legal advice or other expert assistance is required, the services of a competent professional should be sought. The publisher shall not be responsible for any damages resulting from any error, inaccuracy, or omission contained in this publication.

© 2001 by Brownstone Publishers, Inc. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without written permission from the publisher.

PORTABLE COMPUTERS (continued from p. 1)

computer use. Incorporate the text of the agreement into your policy. The Portable Computer Agreement is the heart of your policy and should set out all the specifics on how the employee may use—and may not use—the portable computer [Policy, par. 2].

Policy violations will be disciplined. Make sure employees understand that they'll be disciplined if they violate the policy, says Tomes. Let them know how severe the discipline might be—in our Model Policy, the ultimate discipline is “termination of employment.” The Model Policy also refers to the organization's sanction policy spelling out the disciplinary specifics. If your organization has a sanction policy, you can refer to it in your policy [Policy, par. 3].

What Employee Agreement Should Say

In the Portable Computer Agreement, which forms the heart of the policy, list what the employee may and may not do with the portable computer. The agreement should cover the following, notes Tomes:

Identify computer. Make sure that the computer is identified in the agreement. List the type of equipment and its serial number. If your practice also assigns its own identity number to each piece of equipment, list that number as well, says Tomes. If the employee exchanges the equipment, require that the exchange be logged [Policy, Agr., par. a].

Require employee to safeguard computer. Say the employee must safeguard the equipment and return it upon request or upon termination of his or her employment [Policy, Agr., par. a].

Limit use to business uses. You don't want employees using portable computers for their own personal use. Restrict the use of the computer to business uses. And require the employee to use the computer only for the business uses for which he or she has been trained [Policy, Agr., pars. a and b].

Restrict use to employee. Don't let the employee's friends, family members, or unauthorized fellow employees use the portable computer. Otherwise they could access confidential health information on the computer [Policy, Agr., par. c].

Limit dial-in functions. Allow the employee to dial in only to your practice. You don't want the employee dialing into other services. That could lead to security breaches or to the introduction of viruses into your system. You also don't want an employee visiting porn sites and putting your practice at risk of a sexual harassment lawsuit if the sites are seen by another employee, advises Tomes [Policy, Agr., par. d].

Bar unauthorized software. Another important protection against computer viruses is to bar the employee from introducing unauthorized software into the portable computer, says Tomes. So bar the employee from downloading any software at all onto the portable. Let only designated individuals—in our Model Policy, the compliance officer—do the downloading. Also, bar the employee from inserting any floppy disks, CDs, or other media into the computer unless authorized by the person responsible for authorizing the employee's use of the computer [Policy, Agr., pars. e and f].

(continued on p. 5)

MODEL POLICY

Set Requirements for Appropriate and Secure Use of Portable Computer

Here's a Model Policy instructing employees (and independent contractors and others) on how they may use portable computers your practice issues to them. The Model Policy is adapted from a policy created by health information attorney Jonathan Tomes. That policy appears in his book *The Compliance Guide to HIPAA and the HHS Regulations*, published by Veterans Press of Overland Park, Kans.

The Model Policy begins by explaining why it's needed. It

requires employees to get written authorization for use of a portable computer (par. 1). It requires employees receiving a portable computer from your organization to first sign an agreement on portable computer use (par. 2), and it notifies employees that they are subject to discipline for violating the policy (par. 3). It also contains a copy of the agreement that they must sign.

Talk to your attorney about adapting this policy for use at your health care organization.

PORTABLE COMPUTER POLICY

XYZ Radiology has adopted this Portable Computer Policy to comply with:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- The requirement of the proposed HIPAA security regulations to protect the security of electronic health information; and
- Our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements.

All personnel of XYZ Radiology who use a laptop, notebook, or other portable computer and any equipment associated with its use must be familiar with the policy. Demonstrated competence in the requirements of the policy is an important part of the responsibilities of all XYZ Radiology personnel.

ASSUMPTIONS

- Portable computers pose a significant security risk because they may contain confidential patient information and, because of their portability, they have a higher risk of loss, theft, or other unauthorized access than the practice's nonportable computers.
- Portable computers may be more vulnerable to viruses and other similar threats because the user may not regularly use virus protection software and other electronic safeguards the way the practice does on its network.
- Portable computer use is more difficult for the practice to audit; thus security breaches may be more difficult to identify and correct.

POLICY

1. **General Policy.** Officers, agents, employees, contractors, and others using portable computers must read and understand and comply with this policy. No person may use a portable computer for XYZ Radiology's business purposes or for any purpose, download, maintain, or transmit confidential patient or other information onto a portable computer without the written authorization of the Compliance Officer upon the recommendation of that user's department head.
2. **Right of Use Conditioned Upon Agreement.** The right of any person to use an XYZ Radiology portable computer is conditioned upon agreement to and signature of the Portable Computer Agreement, which appears below.
3. **Enforcement.** All supervisors are responsible for enforcing this policy. Anyone who violates this policy is subject to discipline up to and including termination of employment in accordance with XYZ Radiology's Sanction Policy.

(continued on p. 4)

PORTABLE COMPUTER AGREEMENT

I, *[insert name of individual]* (hereinafter "User") hereby agree to the following:

a. **User's Responsibility for Portable Computer.** XYZ Radiology has issued the portable computer equipment listed below to User for the uses for which User has been specifically trained. Any equipment exchanged must be logged in the equipment log. User's responsibility for the initial equipment provided extends to the equipment listed below and/or any exchanged or additional equipment XYZ Radiology may provide User during User's employment (hereinafter collectively referred to as "Portable Computer"). The Portable Computer and all related components and data are the property of XYZ Radiology and must be safeguarded and returned upon request and upon termination of User's employment.

Equipment	Serial #	Facility Asset #

- b. **Business Use Only.** User will use the Portable Computer solely for XYZ Radiology's business purposes and not for the personal use of User or any other person or entity.
- c. **Use Restricted to User.** User will not permit anyone else including but not limited to User's family and/or associates, patients, patient families, or unauthorized officers, employees, and agents of XYZ Radiology to use the Portable Computer for any purpose.
- d. **Dial-in Functions.** Dial-in functions are restricted to dialing into XYZ Radiology. User is not permitted to dial into any other unauthorized service, Internet service provider, or any other Internet access or to use the dial-up capabilities in any other manner than as instructed. User understands that the hardware has been disabled from performing any functions other than those intended for business use and that User may not attempt to enable such other functions.
- e. **Software Downloading Restricted.** User will not download any software onto the Portable Computer except as downloaded by the Compliance Officer.
- f. **Insertion of Media into Computer.** User will not insert any floppy disks, CDs, or other media into the portable computer without the written authorization of the Compliance Officer.

- g. **Batteries and Cable.** User will use only batteries and power cables provided by XYZ Radiology and will not use other power sources—for example, a car adapter power source.
- h. **Additional Peripherals.** User will not connect any additional peripherals (keyboards, printers, modems, etc.) to the portable computer without the written authorization of the Compliance Officer.
- i. **Securing of Portable Computer.** User is responsible for securing the Portable Computer and all data within his or her home, car, and other locations as instructed in the training provided.
- j. **Locking Cable.** User will use the cable provided to lock the portable computer to immovable objects at all times except when transporting it.
- k. **Leaving Portable Computer Unattended.** User will not leave the Portable Computer unattended unless it is in a secured location.
- l. **Leaving Portable Computer in Car.** User will not leave the Portable Computer in cars or car trunks for an extended period in extreme weather (heat or cold) or in exposure to direct sunlight.
- m. **Carrying Case Required.** User will place the Portable Computer in its proper carrying case when transporting it. The case must display the user's name and identify XYZ Radiology.
- n. **Serial and Asset Numbers.** User will not alter the serial numbers and asset numbers of the Portable Computer.
- o. **Password Usage.** User will not share his or her password with any other person and will safeguard such password and will not write it down so that an unauthorized person can obtain it.
- p. **Maintenance of Patient Confidentiality.** User will maintain patient confidentiality when using the Portable Computer as specified in XYZ's Workstation Policy. User will protect the screen from viewing by unauthorized personnel, and User will properly log out and turn off the Portable Computer when it is not in use.
- q. **Reporting of Loss, Damage, or Security Breach.** User must immediately report any lost, damaged, malfunctioning, or stolen Portable Computer or any breach of security or confidentiality, including any breach of password security, to the Compliance Officer.

User signature _____ Date _____

User title _____

Witness _____

PORTABLE COMPUTERS (continued from p. 2)

Bar unauthorized peripherals.

You don't want the employee to connect anything to the portable computer (batteries, cables, keyboards, printers, and so on) that could cause a system failure because of incompatibility, advises Tomes [Policy, Agr., pars. g and h].

Set rules for securing computer.

To reduce the risk of theft, make the employee responsible for securing the computer within his or her home, car, and other locations. Also, require the employee to use a locking cable that you'll provide to secure the portable computer to an immovable object when it isn't being moved [Policy, Agr., pars. i and j].

Bar leaving the computer unattended. Again, to cut the risk of theft, bar the employee from leaving the computer unattended, unless it's in a secured location. And to avoid damage, bar the employee from leaving the computer in a car or car trunk for an extended period of time in extreme weather and from exposing it to direct sunlight [Policy, Agr., pars. k and l].

Set "in transit" rules. To protect the portable computer from damage, require the employee to use its proper carrying case when moving it, says Tomes. And require the case to have the names of the employee and your organization. This increases the chance that the computer will be returned if it's lost, notes Tomes [Policy, Agr., par. m].

Bar changes to serial numbers and asset numbers. Bar the employee from altering the portable computer's serial number or asset number. You want to always be able to identify the portable computer [Policy, Agr., par. n].

Remind employee of password rules. You'll probably have a separate policy on password usage. But it doesn't hurt to include a general reminder that the employee must safeguard passwords and report any breach of password security [Policy, Agr., pars. o and q].

Require confidentiality to be maintained during use. You'll probably have a separate workstation policy on confidentiality that you can refer to. But remind the employee to

protect the portable computer's screen from view when working and to properly log out [Policy, Agr., par. p].

Require reporting of security breaches. Require the employee to report any security breaches involving the use of the computer. Also, require reporting of any loss, damage, malfunction, or theft of the computer. Have the employee report security breaches to a designated person—in our Model Policy it's the compliance officer [Policy, Agr., par. q].

Have Employee Sign Agreement

Make sure each employee signs the agreement before a portable computer is given to him or her. Have a witness sign the agreement as well. That will provide you with evidence that the employee knowingly signed the agreement, if a dispute ever arises. ■

Insider Source

Jonathan Tomes, Esq.: Tomes & Dvorak, 7111 W. 98th Terr., Ste. 140, Overland Park, KS 66212.

IN THE NEWS

HCFA Expands PET Scan Coverage

On April 10, HCFA issued a program memorandum to its carriers and intermediaries that expands the Medicare coverage of and changes the billing requirements for positron emission tomography (PET) scans. The expanded coverage for PET scans takes effect for services provided on or after July 1, 2001, and the billing changes affect claims received by carriers and intermediaries on or after July 1, 2001. We'll explain the changes and how they might affect your practice.

HCFA Expands Reimbursement of PET Scans

PET scans are very useful for determining the stage of tumor activity in certain cancers and for evaluating certain cardiac and brain activity, says Georgia health care consultant Melody Mulaik. In the past, Medicare has reimbursed PET scans only in very limited circumstances. But even though the recent program memorandum said that HCFA would expand Medicare coverage of PET scans, there are

still significant limits on the circumstances under which they'll be reimbursed, Mulaik notes. According to the program memorandum, Medicare will reimburse PET scans performed on or after July 1, 2001, in the following circumstances:

- Diagnosis, initial staging, and restaging of nonsmall cell lung cancer (NSCLC);
- Diagnosis, initial staging, and restaging of colorectal cancer;

(continued on p. 6)

IN THE NEWS (continued from p. 5)

- Initial staging and restaging of both Hodgkin's and non-Hodgkin's lymphoma;

- Diagnosis, initial staging, and restaging of melanoma (but not for evaluation of regional nodes);

- Diagnosis, initial staging, and restaging of esophageal cancer;

- Diagnosis, initial staging, and restaging of head and neck cancers (but not for central nervous system or thyroid cancers);

- Determination of myocardial viability when a SPECT (single photon emission computed tomography) is inconclusive; and

- Presurgical evaluation of patients with refractory seizures.

Limitations on Reimbursable PET Scan Use

However, Medicare will reimburse the PET scan only when it's used to diagnose cancers and stage and restage tumors in certain ways.

Diagnosis. The program memorandum permits reimbursement for a PET scan's use in diagnosis in only two clinical situations:

- 1) When the PET scan results may assist the physician in avoiding an invasive diagnostic procedure; or

- 2) When the PET scan results may help determine the exact location on the body where an invasive diagnostic procedure should be performed.

Staging. The program memorandum limits when a PET scan used to determine the stage of a cancer is reimbursable under Medicare to these specific situations:

- When the standard imaging study (computed tomography, MRI, or ultrasound) doesn't conclusively determine the stage of the cancer, or when the PET scan could replace one or more of the conventional imaging studies typically used if the conventional study wouldn't be expected to provide adequate information to clinically manage the patient; *and*

- When clinical management of the patient depends on the stage of the cancer identified.

Restaging. A PET scan used for restaging cancers will be reimbursable under Medicare only after the completion of treatment and only to:

- Detect residual disease;
- Detect suspected recurrence; or
- Determine the extent of a known recurrence.

Insider Says: Screening PET scans (those used for testing patients without specific symptoms) aren't reimbursable under Medicare. Neither are PET scans used to monitor tumor response during treatment, Mulaik notes.

Changes in Billing Requirements

The program memorandum contained two billing changes:

Modifiers. Until now, claims for Medicare reimbursement for the professional component of PET scans, or for PET scans performed at free-standing facilities, had to be submitted using modifiers designated exclusively for PET scan claims, Mulaik explains. But according to the recent program memorandum, those modifiers will be eliminated. So

don't include a PET scan modifier on claims the carrier or intermediary will receive on or after July 1, 2001, she says.

Documentation. In the past, carriers and intermediaries have usually required PET scan providers to give additional supporting documentation along with claims for PET scan reimbursement. But the program memorandum says that carriers and intermediaries no longer must require the PET scan provider to submit this additional documentation. Still, the program memorandum requires the PET scan provider to maintain the treating physician's referral on file in the patient's record as well as documentation that the PET scan:

- Was conducted using only FDA-approved drugs and devices; and

- Didn't involve investigational drugs.

The program memorandum also requires the treating physician to certify the medical necessity of the PET scan and to maintain documentation in the patient's medical record to support his or her referral to the PET scan provider.

Insider Says: To obtain a copy of the program memorandum, go to <www.hcfa.gov>. Click on "information for providers," and under "publications" click on "program memoranda and transmittals." Look for Transmittal AB-01-54, April 10, 2001, "Expanded Coverage of Positron Emission Tomography (PET) Scans and Related Claims Processing Changes." ■

Insider Source

Melody Mulaik, MSHS, CPC: President, Coding Strategies Inc., 168 N. Johnston St., Ste. 103, Dallas, GA 30123.

PLUGGING LOOPHOLES

Make Sure Exclusive Contract with Hospital Is Really Exclusive

When you sign an exclusive contract with a hospital, you probably expect that your radiology group will provide all the hospital's radiology services. But you could be in for an unpleasant surprise. Other specialists may take on some of the work you expected to do or some of the patients you expected to serve. And nothing in your contract with the hospital may help you stop this. The result in either situation: You don't get the benefit of the deal you thought you made, warns Virginia health care attorney Thomas W. Greeson.

To help you avoid a similar situation, we'll explain two ways in which the hospital can undercut—or let other specialists undercut—the exclusive aspect of a contract. We'll also tell you about changes that you can seek during contract negotiations to help you prevent this. And we'll give you Model Contract Language you can use as a starting point in your negotiations.

Two Problems to Watch Out For

There are two problems that radiologists with an exclusive contract should be aware of, to prevent unexpected competition and protect the value of their contract, notes Greeson. First, despite your exclusive contract, other specialists may start to move in on your territory. For example, surgeons or cardiologists often perform certain interventional or nuclear imaging procedures—they may even have certification to use the specialized equipment and techniques. If the hospital permits this, the value of your exclusive contract diminishes, says Greeson.

Another possible problem, says Greeson, is that despite the exclusive contract with you, the hospital may open an off-site clinic or imaging center and hire another group to staff it. If your contract doesn't anticipate this possibility, you may be stuck with a less attractive patient population and be denied opportunities to expand the services your group provides.

Hospitals Will Negotiate

You don't have to just accept a raw deal, Greeson emphasizes. Hospitals are usually willing to negotiate your "turf." But it's up to you to make sure the hospital knows precisely what you expect your exclusive contract to cover and to propose protections for your group. Greeson says that a hospital will often accept these protections if you insist on them, but it won't offer them to you out of the kindness of its heart.

Protect Against Poaching by Specialists

Here are two alternatives that could help you if other specialists try to poach on your territory:

Define exclusive radiology services. Have the contract define the services that the radiologists in your group will perform and say that your group has the exclusive right to do them. *Be sure the contract also gives your group the exclusive right to offer any new radiology services.* Then, for example, if the hospital allows a cardiologist to do a nuclear cardiology procedure that your group has contracted to do, you can sue the hospital. You probably won't ever have to enforce this right in court, says Greeson. To protect itself, the hospital will almost certainly develop

a policy that permits only radiologists to do those procedures.

Consider adding the following language, suggested by Greeson, to your contract:

Model Contract Language

- a. Hospital shall not permit Radiology Services or Additional Radiology Services, as those terms are herein defined, to be performed unless performed by, or under the supervision of, a member or employee of Radiology Practice, provided, however, that Radiology Practice may decline to offer any Additional Radiology Service(s) at its discretion, and in that event Hospital may recruit a qualified physician to provide such Additional Radiology Service until such time as Radiology Practice is willing to provide such Additional Radiology Service(s).
- b. Radiology Services means all procedures performed at Hospital which involve ionizing radiation, ultrasound, or magnetic resonance imaging for any diagnostic or therapeutic purpose. Radiology Services shall include Additional Radiology Services.
- c. Additional Radiology Services means any procedures which, due to technological advances or progress in the state of the art, supplement or replace, in whole or in part, any Radiology Service.

Limit credentialing. Another way to achieve the same end is to have the hospital agree that it won't grant medical staff privileges—or credential—anyone else to do any procedure that the hospital has credentialed the members or employees of the radiology group to do. You avoid defining radiology services and make the arrangement more flexible, which you or the hospital may prefer.

(continued on p. 8)

PLUGGING LOOPHOLES

(continued from p. 7)

Consider including the following language in your contract:

Model Contract Language

Hospital shall not grant any physician who is not a member of, or employed by, Radiology Practice privileges to perform any services or procedures members and/or employees of Radiology Practice are credentialed to provide.

Protect Against Off-Site Hospital Locations

To help you keep the hospital from setting up competing facilities, make sure your exclusive contract covers not only the hospital but any off-site locations where the hospital currently

offers radiological services. You also may want the right to provide services at any facilities the hospital opens or acquires in the future—or to decline that work if the group prefers. In other words, you want the “right of first refusal”—the right to get first crack—at providing services in new facilities.

Don't assume you have any of those rights unless the contract spells them out, Greeson cautions. If you want those rights, he suggests you try to add the following language to your contract:

Model Contract Language

This contract is for Radiology Services provided by Radiology Practice to Hospital in the following locations:

[insert addresses of hospital and of any off-site clinics, imaging centers, or other facilities where Practice expects to provide services]

In the event Hospital opens, acquires, or operates any additional locations, clinics, imaging centers, or other facilities that will offer Radiology Services that members or employees of Radiology Practice are credentialed to perform, Radiology Practice shall have the right of first refusal to provide such Radiology Services. ■

Insider Source

Thomas W. Greeson, Esq.: Reed Smith Hazel & Thomas LLP, 3110 Fairview Park Dr., Ste. 1400, Falls Church, VA 22042.

Understanding Corporate Integrity Agreements

Several years ago the government developed a new weapon for its enforcement arsenal—the corporate integrity agreement. It was originally intended for use against large corporations that had committed Medicare fraud or abuse, as an alternative to the government putting the company out of business. But the government recently started insisting on using these agreements even when it settles fraud or abuse issues with small health care providers, says Philadelphia health care attorney Joan Roediger.

A corporate integrity agreement is an “option” the OIG offers to providers settling civil health care fraud and abuse cases to avoid exclusion from the Medicare program. Instead, the provider has the opportunity to continue to treat Medicare patients, as long as it complies with a contract with the OIG requiring it to conduct its business according to certain principles in the contract. That contract is the corporate integrity agreement.

We'll explain the requirements that appear in most corporate integri-

ty agreements. And just in case you ever need them, we'll give you some tips on negotiating a corporate integrity agreement. We'll also point out two major concerns that might make you consider whether staying in the Medicare program under a corporate integrity agreement is worth it (see box on p. 10).

Corporate Integrity Agreement Explained

Corporate integrity agreements are like compliance programs, says Roediger, with a few important differences. The most important difference is that a compliance program is voluntary, and you develop it yourself, considering the needs and resources of your practice. But a corporate integrity agreement is anything but voluntary, says Roediger, and the government's attorneys, with input from you, will decide how it should be structured and how much of your resources you should devote to it. Although there's room for limited negotiation on a case-by-case basis, all corporate

integrity agreements require some common elements:

Training. Corporate integrity agreements are specific about the type and amount of training your employees must have, says Roediger. Recognize that the amount of training the OIG thinks your employees need may be more than you think they need or want to pay for.

Auditing. Corporate integrity agreements always provide for stringent auditing, usually conducted periodically by an independent review organization, like an accounting firm. “If you have a corporate integrity agreement, face it—for the next several years the auditors are going to be a part of your life,” Roediger remarks. And you must pay for them. But, if your practice already has good in-house auditing capabilities, it doesn't hurt to ask whether you can conduct the audits yourself, rather than use an independent review organization.

Monitoring. The OIG may also require that an independent review organization monitor your practice,

Roediger says. That's to make sure you have systems operating properly to prevent a recurrence of whatever got you into trouble in the first place, she explains. (It may be the same company that's providing the auditing services, or it may be another one—it depends on what the OIG thinks your problem areas are.) Just like the auditors, these monitors will be around a lot. And they're required to report to the OIG if they notice any problems in your practice. Plus the OIG can penalize you if it decides that the independent review organization isn't doing its job properly.

Reporting. Corporate integrity agreements always include strict reporting requirements. Not only will your independent review organization have to report about your activities, but you'll have to prepare reports as well, says Roediger. In general you'll have to:

- Identify your compliance officer;
- Establish that he or she is a high-level employee;
- Certify that all the training you're required to provide to your employees has been completed; and
- Certify that you're complying with applicable laws, rules, and regulations.

And depending on how you landed in hot water in the first place, your corporate integrity agreement may include other, sometimes substantial, reporting requirements.

Penalties. Your corporate integrity agreement is a contract and so it will contain penalties if you violate it, Roediger says. Typically the penalties are fines ranging from \$1,500 to \$2,500 per day for a violation of the agreement. Plus, if the OIG thinks you're not following the corporate integrity agreement, it may set it aside and exclude you from the Medicare program. If that happens, Roediger notes, the government may reopen its investigation of your prac-

tice and come after you for more money—and perhaps even file criminal charges.

Negotiating Corporate Integrity Agreement

With luck, you'll never have to negotiate a corporate integrity agreement. Practicing under one is a big burden, and it will be years before things return to something like normal. In fact, things will never be the same. But, if you're in trouble with the government, a corporate integrity agreement may be better than exclusion—at least you'll stay in business and can continue to treat your Medicare patients. Roediger suggests you keep the following in mind if you're ever in that unfortunate situation:

Get good advice. You can't do it alone. Get the best health care attorney you can find to advise you on the financial and practical implications of this agreement for you, and ask the attorney to hire an auditor to negotiate the auditing provisions of the agreement, Roediger says. (It's best for the attorney to hire the auditor because you stand a better chance that the communications you and the attorney have with the auditor will be protected from public disclosure by the attorney-client or attorney work product privilege, Roediger explains.)

Take a cooperative attitude. The OIG views its corporate integrity agreements as educational tools, not punishment. If the OIG believes you want to improve your operations and are willing to learn from the process, the OIG is more likely to listen to your concerns. That means, you may be in a better position to protest if the OIG wants to impose requirements that won't work for you on an operational level or don't address the issues that caused your troubles.

Keep expectations reasonable. You have to accept that operating under a corporate integrity agree-

ment is going to cramp your style in some ways. Rather than protesting everything in the agreement, Roediger suggests, think hard about where the heaviest administrative burdens are likely to fall, and try to negotiate for less onerous conditions in those areas. Also, keep in mind that the corporate integrity agreement is all about teaching you how to conduct your business in a compliant manner. The OIG is more likely to listen to suggestions that foster practical knowledge and compliance after the agreement ends, she says.

Here's a look at the negotiability of the corporate integrity agreement's common requirements, based on Roediger's experience:

► **Training.** There's sometimes a little room to negotiate the training issue, but not much. The OIG will insist on comprehensive training in compliance. And you should think of this as an opportunity to improve your staff—and make the best of it. There may be some flexibility on the amount of training you must give in specific areas, such as billing and coding, to employees whose job functions don't include that area.

► **Auditing.** Close auditing by an outside firm is likely, Roediger says, but you may be able to include your internal accounting or auditing staff in the process. You may want to propose to the OIG—as an educational opportunity—that the auditors train your staff to conduct internal audits. Then, when the corporate integrity agreement has expired, you'll have trained staff to conduct ongoing internal auditing and monitor billing compliance, Roediger points out.

► **Monitoring.** If the OIG wants your practice to have a monitor, you'll have a monitor. But you may be able to negotiate a little about what the monitor is there to look for, and the methods it uses to assess

(continued on p. 10)

CORPORATE INTEGRITY AGREEMENTS (continued from p. 9)

whether you're following the corporate integrity agreement. Try to negotiate for monitoring methods that disrupt the way you normally do business as little as possible, Roediger says. While it's important that your practice remain compliant with the corporate integrity agreement, you need to focus on how you can work cooperatively with the monitor.

► **Reporting.** Most elements of the reports you must make to the OIG under the corporate integrity agreement are nonnegotiable, Roediger says. But in some corporate integrity agreements the government will ask you to report whenever you open a new office, change the business name, add a new partner, and so

on. You want to try to negotiate out some of these requirements if they would pose a business handicap, Roediger says. Instead, you could offer to report those events in your regular reports to the OIG.

You may also want to try to negotiate the confidentiality of your reports to the OIG. The OIG can't promise you confidentiality for them. But it *might* agree to protect the confidentiality of a report you submit if you can show that the report is very sensitive. If you can't get that promise, try to get the OIG to agree to notify you if it gets a Freedom of Information Act (FOIA) request for information you provided under your corporate integrity agreement. Although there's not much you can

do to prevent the release of your sensitive information if someone submits a FOIA request, at least if you have advance warning you can be ready to do some spin control, Roediger says.

► **Penalties.** As far as the OIG is concerned, you're already getting a break by not being thrown out of the Medicare program. So don't expect much flexibility on penalties, Roediger says. But, if your practice is financially strapped, you may be able to get the OIG to agree to penalties at the low end of the typical range, she says. ■

Insider Source

Joan Roediger, Esq.: Obermayer Rebmann Maxwell & Hippel, LLP, 1617 John F. Kennedy Blvd., 19th Fl., Philadelphia, PA 19103; <joan.roediger@obermayer.com>

► *Special Risks of a Corporate Integrity Agreement*

Before you agree to sign a corporate integrity agreement, you should give some thought to a couple of special risks, says Roediger. Depending on the needs and circumstances of your practice, you may decide that you would rather be excluded from Medicare than accept a corporate integrity agreement. Here are the two special risks to consider:

QUALITY OF CARE MONITORING

If you decide to go forward with a corporate integrity agreement, the government may decide to look closely at your practice of medicine, not just at your Medicare billing practices. Last September, the OIG posted its corporate integrity agreement with the Vencor Corporation on its Web site. This agreement is significant, Roediger explains, because it's the first one to include specific provisions for monitoring a provider's quality of care. It requires the company to adopt a comprehensive internal quality improvement program that's subject to external monitoring and review. This is an unusual requirement because the OIG's authority extends only to enforcing laws and regulations about Medicare billing. But the OIG is taking the position that if Medicare is billed for substandard care, then the bill is fraudulent. So the OIG believes it has a right to monitor the quality of the care provided to a Medicare patient.

This opens the door to second-guessing medical decision making, Roediger says. Although the Vencor agreement requires only an independently monitored quality improvement system, it's possible that some future corporate integrity agreement could impose direct monitoring of medical care, quality, and decision making. Providers of all kinds should be disturbed at this develop-

ment, Roediger says, given the current risks of malpractice lawsuits and the large rewards collected by some whistleblowers. Besides the annoyance of having your medical decisions second-guessed, any report that indicates you don't provide top quality care 100 percent of the time could have serious implications for your practice, Roediger says.

LOSS OF CONFIDENTIALITY

There's a risk that a corporate integrity agreement, and the reports you must file to comply with it, could be made public. As a government agency, the OIG is subject to the Freedom of Information Act, Roediger cautions. That means that if someone requests the reports you prepared to comply with the corporate integrity agreement, the government will probably have to release them. That's a bad situation for you, because the reports for corporate integrity agreements often contain extremely private and sensitive information.

You can raise this concern with the OIG attorney when you're negotiating your corporate integrity agreement, Roediger suggests. There's a provision in FOIA that may allow the government to withhold release of a document if its release would have a "chilling effect" on securing the cooperation of others or the enforcement of laws, she says. But, in general, Roediger says, you should be prepared that any report you give to the government may eventually be made public. At the same time, keep in mind that failure to report thoroughly and accurately will result in penalties, exclusion, and perhaps repayment demands and possible criminal charges.