

# THE PHYSICIAN'S COMPLIANCE ALERT™

PROVIDING PHYSICIANS WITH MEDICAL PRACTICE COMPLIANCE SOLUTIONS

## HIPAA Security Rule Catching Many Medical Practices Off Guard

A doctor's office is an ideal place to steal a person's identity. "In most practices, folders and files are everywhere, including those brackets outside exam rooms. What a perfect setting for an identity thief to steal patient information," reveals Johann F. Lee, consultant and owner of Decitech Services, a consulting firm located in Lawrenceville, NJ. Other security weak spots can lead to equally hair-raising outcomes. "The potential certainly exists for someone without authorization to get into a computer system and change patient data, such as diagnoses or lab results," comments Landon T. Futch, owner of Essential Solutions, LLC, a business consulting firm based in Baton Rouge, La.

Under the Health Insurance Portability and Accountability Act of 1996

(HIPAA) Security Rule, which went into effect just this past April 20, security violations such as these are punishable by fines of up to \$25,000 and 10 years in prison. Participation in Medicare and Medicaid may also be at risk if providers are not HIPAA-compliant.

The goal of the Security Rule is to protect the confidentiality, integrity, and availability of certain protected health information (see HIPAA Security Rule Terms, page 6). But are physicians' practices ready?

"Most practices have gotten the HIPAA privacy piece right, but not the security piece," observes Futch. "I find that many doctors and office managers mistakenly believe that the privacy measures they have taken also cover the security requirements. Or they think they are completely safe because they have only one terminal on the Internet and there is no protected health information on it." But what about the person who is fired and still has the password? What if the water sprinkler system is activated and the entire system is ruined? Backup tapes are often several years old and may not even be viable.

### Halfhearted effort

In fact, a recent survey from the Healthcare Information and Management Systems Society showed that only 50% of covered entities are ready for the HIPAA Security Rule,

notes John C. Parmigiani, independent consultant and Senior Vice President for consulting services for Quick Compliance, in Avon, Conn.

"HIPAA led to a lot of paperwork, but I think we're basically back where we started from in terms of security and privacy," Lee sadly points out. "The biggest dangers may not be electronic, but rather the paperwork that is left everywhere. You have to look at the paper flow in your practice. Physicians may think that no one cares whether a patient had stitches, for example, but what about the demographic data in the office?"

Another common misconception occurs when a practice assumes it is compliant with the Security Rule because it leases services from a software company, says Rhonda Picou, RN, MSN, CPC, vice president of physician compliance for Peak Performance Physicians, LLC, based in New Orleans. "Even in that case, you still need to have the policies and procedures in place and perform the required risk assessments."

Most dangerous of all, perhaps, is that those in doctors' practices and even hospitals believe they are "under the radar" when it comes to security regulations. "This belief is partly correct," notes Parmigiani. HIPAA is an unfunded mandate and is handled very benevolently by the government,

(Continued on page 6)

### CONTENTS

#### Editorial

Running the Numbers .....2

#### Coding

What Is Your Diagnosis?

A Look at the Revised

ICD-9-CM Guidelines .....3

#### Billing

Rounds and Revenue:

Billing for Hospital Visits .....5

**Running the Numbers**

Physicians are inundated with statistics, but here is one that pertains to the health of your business, not your patients. Although the Health Insurance Portability and Accountability Act of 1996 Security Standards were just implemented on April 20, of this year, a recent survey from the Healthcare Information and Management Systems Society showed that just one half of covered entities are prepared to comply, according to this month's cover article. If your practice is like most, you probably depend on a software vendor to shield patient information but myriad details require your attention and far too many to address in a single issue. For example, who has the passwords to your computerized patient information? Does your computer have an anti-virus program? We recently reviewed a large medical practice that did not have this crucial tool—and data was not regularly backed-up at an off-site location. A Web-wise intruder could devastate those records. If you want to see where you stand security-wise, we would be pleased to provide a sample implementation manual on request.

Just as essential a topic is coding compliance. The Office of the Inspector General of the US Department of Health and Human Services is investigating a number of your coding practices, as noted in its Fiscal Year (FY) 2005 Work Plan. And it has much incentive. The FY 2004 Improper Medicare Fee-For-Service Payment Report states that the Centers for Medicare and Medicaid Services intended to shrink its net rate of improper payments to 4.8%; in fact, the rate was 9.8% for FY 2004. Insufficient documentation accounted for 43.7% of errors, followed by nonresponse (29.7%), medically unnecessary claims (17.2%), incorrect coding (7.7%), and other mistakes (1.6%).

With this in mind, we address two other important areas this month: the revised ICD-9-CM Official Coding Guidelines and coding for hospital visits. Excluding nonresponse claims, 26.8% of claims for initial hospital visits were said to have been paid in error; the same is true for 24.3% of claims for subsequent hospital visits. We want to help you ensure that your own claims are indisputable.



John W. McDaniel  
 Editor-in-Chief  
 Toll-free phone: 1-800-764-2633  
 E-mail: [jmcdaniel@premierhealthcare.com](mailto:jmcdaniel@premierhealthcare.com)

Randall D. Ayers, MD  
 Clinic for Rheumatic Diseases  
 Tuscaloosa, Ala.

Michael W. Carbrey  
 Health Care Consultant  
 Celebration, Fla.

Robert J. Chugden, MD  
 West Jefferson Emergency  
 Physicians Group  
 Marrero, La.

Charles E. Colitre  
 President  
 Med-Management Group, Inc.  
 Akron, Ohio

Randy J. Gershwin, MD  
 Medical Director  
 Community Practice  
 Lutheran Hospital  
 Brooklyn, NY

Sara S. Grostick, MA, RHIA  
 Director and Associate Professor  
 Health Information  
 Management Program  
 University of Alabama at Birmingham  
 Birmingham, Ala.

D. Scott Jones, CHC  
 Vice President, Risk Management  
 InLight Risk Management  
 Oklahoma City, Okla.

Harold B. Kaiser, MD  
 Allergy & Asthma Specialists, PA  
 Minneapolis, Minn.

Thomas Loughrey, MBA, CCS-P  
 Chairman and CEO  
 Economedix, LLC  
 Orange, Calif.

Rhonda Lynn Picou,  
 RN, MSN, CPC  
 Vice President, Physician Compliance  
 Peak Performance Physicians, LLC  
 New Orleans, La.

**Editor**

Cynthia Starr, MS, RPH  
 Phone: 201/652-6181  
 E-mail: [cstarr@premierhealthcare.com](mailto:cstarr@premierhealthcare.com)

**Publisher**

Premier Healthcare Resource, Inc.  
 150 Washington St.  
 Morristown, NJ 07960  
 Phone: 888/457-8800  
 Fax: 973/682-9077  
 E-mail: [publisher@premierhealthcare.com](mailto:publisher@premierhealthcare.com)

This newsletter is published by Premier Healthcare Resource, Inc., Morristown, NJ.

© Copyright strictly reserved. This newsletter may not be reproduced in whole or in part without the written permission of Premier Healthcare Resource, Inc. The advice and opinions in this publication are not necessarily those of the editor, advisory board, publishing staff, or the views of Premier Healthcare Resource, Inc., but instead are exclusively the opinions of the authors. Readers are urged to seek individual counsel and advice for their unique experiences.

# What Is Your Diagnosis? A Look at the Revised ICD-9-CM Guidelines

At this point, you might think that the Health Insurance Portability and Accountability Act (HIPAA) has become the center of a regulatory solar system with so many of your routine tasks now revolving around its many tenets. That ever-present acronym can now be found in still another place: the recently modified ICD-9-CM Official Guidelines for Coding and Reporting. The latest version went into effect on April 1 of this year.

Among various changes is a new stipulation that adherence to the guidelines when assigning ICD-9-CM diagnosis and procedure codes is required under HIPAA. The diagnosis codes are to be used in any healthcare setting; the procedure codes signify inpatient procedures billed by hospitals. Generally, the guidelines remain a work in progress. In reading through the document, you will see that a number of its many short chapters have yet to be written. For example, there is currently no guidance for the use of ICD-9-CM codes describing mental disorders (290 through 319); diseases of the digestive system (520 through 579); diseases of the skin and subcutaneous tissue (680 through 709); and diseases of the musculoskeletal and connective tissue (710 through 739). In its place is the notation “reserved for future guideline expansion.”

This time around, the Centers for Medicare and Medicaid Services and the National Center for Health Statistics have provided direction in several areas not addressed in the previous two incarnations, including coding for diagnoses of diabetes mellitus (DM); cerebrovascular accident (CVA); chronic obstructive pulmonary disease (COPD) and asthma; COPD and bronchitis; and toxic effects induced by ingestion of a harmful material. More detailed explana-

tions have been presented in other sections; a notable example is the discussion of sepsis in the chapter on infectious and parasitic diseases. As is so often the case, two of the latest inclusions reflect evolving medical opinion and technologic advances—the guidelines explain how to select diagnosis codes when patients undergo prophylactic organ removal to prevent a primary malignancy or a metastasis and when in utero surgery is performed on a fetus. While there are too many aspects to cover in this article, here are a few essential points.

## **COPD and asthma**

The guidelines note that it can be difficult to split apart the components of COPD and asthma, and as a result, the conditions for which the patient is being treated can be described in any number of ways. But as always, your choice of code must be reflected by the terms used in your patient's chart. A good practice when making a selection, according to the guidance, is to first examine the index and the codes in the tabular list, without overlooking any instructional notes.

COPD comprises obstructive chronic bronchitis, code subcategory 491.2 and emphysema, code 492—and each of these is further divided. Obstructive chronic bronchitis can be coded as 491.20, without exacerbation, or

491.21, with (acute) exacerbation. The latter, a worsening of the chronic disorder, should be distinguished clearly from acute bronchitis in your patient notes. Acute bronchitis, code 466.0, stems from infection, the guidelines state. However, the patient who develops acute bronchitis in conjunction with COPD is described with code 491.22. Of course, a case of acute bronchitis could lead to a subsequent acute exacerbation. But even in that situation, you would code the diagnosis as 491.22, because at least code-wise, acute bronchitis supersedes an acute exacerbation of chronic bronchitis. If the documentation is too vague to establish what kind of COPD a patient has, use code 496, which signifies chronic airway obstruction, not elsewhere classified.

Asthma and its permutations are found in the 493 series of codes, which is partitioned into 493.0, extrinsic asthma; 493.1, intrinsic asthma; 493.2, chronic obstructive asthma; 493.8, other forms of asthma; and 493.9, asthma, unspecified. A fifth digit is required for all of these except 493.8. A “0” indicates an unspecified code; in other words, you don't have sufficient detail to supply a more precise ICD-9-CM code. Insert a “1” in the fifth digit to signify “with status asthmaticus”; a “2”, “with (acute) exacerbation.” In the coding hierar-

*(Continued on page 4)*

chy, status asthmaticus is the primary diagnosis when documented concurrently with COPD or acute bronchitis. Similarly, when status asthmaticus is noted in the chart along with an acute exacerbation of asthma, the status asthmaticus is the prevailing condition. Choose a single code that best describes the patient's form of asthma and insert a "1" as the fifth digit in the code. For example, if an acute exacerbation of chronic obstructive asthma has deteriorated into status asthmaticus, the proper code is 493.21.

### Diabetes mellitus

ICD-9-CM coding for DM, which relies on the 250 series of codes, can be intricate. The first thing you have to remember is to add a fifth digit to each of the codes to identify the type of disease. A "0" indicates DM, type 2 or unspecified type, not stated as uncontrolled; a "1" denotes type 1 [juvenile type], not stated as uncontrolled; "2" represents type 2 or unspecified type, uncontrolled; and a "3" designates type 1 [juvenile type], uncontrolled. When the type of DM a patient is being treated for has not been documented in the chart, it should be coded as type 2 with a "0" or a "1" in the fifth place, depending on whether it is controlled or not. For example, if the record states only that the patient has uncomplicated DM, the appropriate entry would be 250.00 if it "is not stated as uncontrolled" or 250.01 if it is uncontrolled.

What if the chart notation indicates that the patient has DM that is well-controlled with insulin but doesn't specify whether the disease is type 1 or type 2? By default, you would choose the type 2 code, 250.00, and add the V code, V58.67 for long-term (current) use of insulin. However, you would not attach the V code if you administered an acute dose of insulin during an office visit to push down blood glucose levels.

This category contains the most etiology-manifestation combination codes, according to the guidelines. That is, the code incorporates both an underlying disease and a complication requiring treatment. You would then apply a second code to more fully describe the problem. Consider the patient with uncontrolled insulin-dependent DM and a gangrenous toe. The first code recorded would be 250.73, diabetes with peripheral circulatory disorders (the last digit specifies uncontrolled type 1 disease), and subsequently, 785.4 for gangrene. You would continue in this manner until you have described all of the DM-related disorders for which a patient is being treated. For example, if the aforementioned patient also had polyneuropathy, you would affix code 250.63, diabetes with neurologic manifestations, plus code 357.2, which indicates polyneuropathy.

Pre-existing DM in pregnancy is handled differently—you begin with code 648.0x, with "x" representing a fifth digit, zero through four, which describes the point in the pregnancy during which the encounter took place. The 648 sequence of codes encompasses "other current conditions in the mother classifiable elsewhere, but complicating pregnancy, childbirth or the puerperium." Next, a code from category 250 conveys DM type. Gestational diabetes is indicated by code 648.8x, abnormal glucose tolerance. Keep in mind that the 648 series includes other disorders that make pregnancy more treacherous. For example, 648.1x is thyroid dysfunction; 648.4x, mental disorders.

The guidelines also address insulin pump malfunction. A resulting underdose is first coded as 996.57, mechanical complication due to insulin pump. You would then add a secondary DM code. While 996.57 is also the primary code for an overdose resulting from a

faulty pump, you would need to add two more codes: 962.3, poisoning by insulins and antidiabetic agents and finally, the pertinent 250 code.

### Ischemic stroke

Two brief sections have been added to Chapter 7, Diseases of Circulatory System. One asserts that code 434.91, cerebral artery occlusion, unspecified, with infarction, is a default code for stroke, CVA, and cerebral infarction not otherwise specified. It includes the reminder that code 436 is reserved for acute but ill-defined CVA, and it should not be used when a stroke or a typical CVA has been documented in the patient's chart.

When a cerebrovascular hemorrhage or infarction has been triggered by surgery, the appropriate diagnostic code is 997.02, iatrogenic cerebrovascular infarction or hemorrhage. If you do use this code, your documentation has to explain what the intervention was and how it led to the CVA. You must then add a secondary code to classify the type of stroke the patient has suffered. Appropriate choices are 430, subarachnoid hemorrhage; 431, intracerebral hemorrhage; or 432, other and unspecified intracranial hemorrhage. Or, a code can be selected from one of the subcategories under code 433, occlusion and stenosis of precerebral arteries or code 434, occlusion of cerebral arteries. Either of these options requires that a "1" be used as a fifth digit to indicate cerebral infarction. Do not use code 436 to describe postsurgical CVA.

Review the ICD-9-CM guidelines to sharpen your own documentation skills. Concentrate in areas you tend to most often treat. You can find the entire set at: [www.cdc.gov/nchs/data/icd9/icdguide.pdf](http://www.cdc.gov/nchs/data/icd9/icdguide.pdf).

*Written and reported by Cynthia Starr, editor. For more information on coding, go to our Web site (see page 8).*

# Rounds and Revenue: Billing for Hospital Visits

When selecting a level of service for care rendered to inpatients, you can base your choice on time expended rather than on the scope of history, physical, and medical decision-making. You should consider this option when more than 50% of an encounter is devoted to coordination of care or counseling.

"That will often be the case on a hospital unit," observes Rhonda Lynn Picou, RN, MSN, CPC, vice president of physician compliance for Peak Performance Physicians, LLC, located in New Orleans, La. "Say that you have an elderly man on a course of intravenous antibiotics for several days, and he's getting better, but you still see him daily. He's already been examined thoroughly, so you don't need to do more than listen to his lungs, which does not qualify as an expanded problem-focused examination. In addition, there isn't enough new information for an expanded problem-focused interval history. However, because he has other chronic ailments, you are regularly making moderately complex medical decisions. You confer daily with other practitioners—physicians, nurses, pharmacists—as well as the patient's family. Yet, despite the time needed to guide treatment, you don't meet the requirements for level two subsequent hospital care since you can only document one of the three essential components for this code. In that situation, you might want to use time instead."

Time is measured differently in a hospital than it is in an office setting, Picou explains. Whereas evaluation and management (E&M) codes for

office services are built on care given while face-to-face with the patient or the patient's family, hospital E&M codes incorporate time used for tasks that contribute to the patient's care but are not necessarily performed at the bedside. For example, you would make note of the time utilized on the patient's floor or unit to review the laboratory results or talk to the nurses or other physicians participating in that patient's treatment. The caveat when calculating time dedicated to daily care, though, is that you cannot include periods spent in areas other than the patient's unit.

Here is a very basic illustration: in providing subsequent care to an inpatient, you first spend five minutes performing a cursory physical examination. You then sit down and talk to the patient about her progress and her treatment plan for another 20 minutes. The total encounter is 25 minutes, making the use of a level two code appropriate (see Table). "Some physicians think you compute only

the time spent counseling the patient, but that isn't true," Picou advises. "You bill for the entire length of the visit." By the way, time is not used to bill services provided to patients admitted for observation.

Of course, documentation is essential. Always specify the interval, and describe the coordination of care or counseling that took place. For example, if you evaluate a patient in the morning and then discharge that patient later in the day, you would combine both periods to determine the discharge level. "In most cases, that's going to be more than 30 minutes, and you will select the higher code," Picou says. "But you have to document the duration of both sessions as well as what transpired. You can't just say that you spent 40 minutes with the patient. That way, if you're audited, it's clear that you've met the requirements for the code."

*Reported and written by Cynthia Starr, editor. For more information on coding, go to our Web site (see page 8).*

## Tying Service Level to Time

### Initial hospital care codes

99221 (30 minutes)	99222 (50 minutes)	99223 (70 minutes)
--------------------	--------------------	--------------------

### Subsequent hospital care codes

99231 (15 minutes)	99232 (25 minutes)	99233 (35 minutes)
--------------------	--------------------	--------------------

### Initial inpatient consultations

99251 (20 minutes)	99252 (40 minutes)	99253 (55 minutes)
99254 (80 minutes)	99255 (110 minutes)	

### Follow-up inpatient consultations

99261 (10 minutes)	99262 (20 minutes)	99263 (30 minutes)
--------------------	--------------------	--------------------

### Hospital discharge services

99238 (30 minutes)	99239 (>30 minutes)
--------------------	---------------------

## HIPAA Security Rule Terms

The goal of the HIPAA Security Rule is to protect health information, especially electronic health information. There are three categories of security measures covered by the rule:

- Administrative safeguards are the actions, policies, and procedures that govern the security measures you use to shield electronically protected health information in your practice; the safeguards detail the way you intend to choose, develop, implement, and maintain your security procedures as well as your plan for ensuring that your staff protects data.
- Physical safeguards are the security measures that protect your practice's electronic information systems and any related buildings or equipment from natural and environmental hazards and from unauthorized intrusion.
- Technical safeguards refer to the technology you utilize to guard electronically protected health information and the policy and procedures controlling access to that technology and the ways in which it is to be used.

The rule contains standards and implementation specifications for each category. Standards are less detailed, while implementation specifications give precise methods for complying. Methods are required or addressable. If required, the method must be implemented. If addressable, practices must assess measures and may implement those deemed appropriate. If the measure is not implemented, the practice must document its rationale.

*Note: For more information on the HIPAA Security Rule, go to [askhipaa@cms.hhs.gov](mailto:askhipaa@cms.hhs.gov) or call the CMS HIPAA hotline, 1-866-282-0659. Other useful Web sites are sponsored by the Workshop for Electronic Data Exchange, at [www.wedi.org](http://www.wedi.org) and the Healthcare Information and Management Systems Society (HIMSS), at [www.himss.org/ASP/topics\\_privacy.asp](http://www.himss.org/ASP/topics_privacy.asp).*

he adds. For one reason, the rule is complaint-driven and there are no "security police" out looking for non-compliant practices. "As a result, many covered entities have to convince themselves that compliance is important," he admits.

"The danger will come, however, from a lawsuit or whistle-blower. It may take a high-profile court case to convince people to make the commitment to security," he continues. During discovery in a lawsuit, the opposing attorney would look closely at the process a practice used to ensure protection. "I can envision such a case becoming 60 Minutes material. A case like that could ruin a practice," Parmigiani adds.

Practices must therefore invest the time and resources to protect patient

information-and they must begin soon (see "What the Experts Say," page 7). Doing so may require only minor modifications for some practices. "The HIPAA Security Rule is not designed to make you go broke," comments Parmigiani.

The first step is to perform a risk assessment, then write and implement a risk management plan, urges Picou. This plan must include a contingency and recovery piece for protecting health information. "I've known lots of people who do not back up their laptops, for example," she says. "But computer theft is not rare, and practices must implement a way to automatically back up all of their data. This is true whether or not you have a practice management software program in place."

Even if you do not have electronic medical records, you still need a risk assessment because there is protected health information such as patient names and diagnoses in your computer, comments Picou. "In addition, yearly surveys by the US government will likely include security issues," Futch adds.

For small practices, the risk analysis can be done relatively quickly and easily, Parmigiani predicts. First, look at the computer software and hardware and how the data are collected, stored, and moved. Also, examine who has access and how that access is protected. Then, policies must be written and the staff must be trained. "A 45-minute in-service is usually adequate for the training," he remarks, urging that there should also be sanctions in place for personnel who do not adhere to security policies and procedures. Finally, the practice must take ongoing steps to identify and fix lapses in the practice.

"Overall, the requirements are flexible and you have to look at what you need," Picou says. "If you do not implement a Security Rule measure, however, you must document the reason."

### Get some support

Nearly all practices will require some assistance in meeting HIPAA's security provisions. "The security rule will be harder to address than the privacy piece because of the technology aspect," reveals Picou. One reason is that you can never take a secure network for granted, since computers and computer viruses change continually. "Some practices don't even have up-to-the-moment virus protection, much less firewalls," she says. "For these reasons, I think most healthcare practitioners will have difficulty meeting the rule without external help."

One option is to hire a consultant. "This person would have to return

## What the Experts Say

In many cases, it's the little things that matter most. The commonsense security measures listed here are often overlooked, according to the experts. They suggest you educate your staff on each and every one of the following points:

- Shred all documents that contain protected health information before disposing of them.
- Do not allow everyone to use the same computer password. Leaks from the system can be traced only if different passwords are used.
- Check backup tapes regularly. Old tapes often become unusable.
- Automatically back up electronic data, even from offsite locations such as home computers and laptops. Never keep data exclusively on the server.
- Develop an e-mail policy, including which e-mails can and cannot be opened or sent.
- Never put protected health information in e-mails.
- Never download music or other unnecessary materials. The Web sites may have viruses.
- Determine who has office access and remote access to the system and eliminate access when an employee leaves your payroll.
- Use screen savers and automatic log-offs on computers. Computers should always be turned off when they are not attended.
- Contract with business associates to ensure that data is protected at each site.
- Never open attachments on e-mail from unfamiliar senders.
- Notify the recipient before faxing or e-mailing data.
- Keep fax machines and copiers away from public areas.
- Laptops and palm digital assistants are weak links in the security chain, since they can be discarded, lost, or stolen. Backups should be made regularly, and discarded computers should be cleared of data.
- Home computers used to dial into the system should be equipped with virus protection and firewalls.

periodically because compliance requires continual assessment and action," Picou advises.

Another approach is to purchase or lease a software program and assign specific tasks to various personnel. "There are software programs designed to help with the risk assessment, policies, and procedures, but these must still be installed and completed by someone," she urges. For this, you will need to appoint a HIPAA security officer, a position that is required under the rule. "Don't give this role to someone who already has a full-time job," she recommends. Most staff members will be able to

handle the administrative and physical safeguards that are required, but will probably still need an expert for the technological safeguards. "It is important to give the security officer the adequate time, resources, and support he or she will need," Parmigiani agrees.

He goes on to say that practices with three to five doctors can purchase HIPAA security software tool kits for a few hundred dollars. Software programs are also available for larger practices and are generally much more expensive. "These all come with technical guides, training videos, and other tools," Parmigiani

notes. "And because most practices rely on computer vendors, our software also provides questions pertaining to vendor safeguards."

"We support thousands of providers," says Jeff Hamel, business developer for MEDTRON Software Intelligence Corp. and program manager for MEDDATA Service Bureau, in Covington, La. "Our software is HIPAA-compliant and our clients can be assured their data is safe. He suggests that physicians check with the state Medicare and Medicaid Web sites to ensure that any software company or service bureau is HIPAA-compliant.

Software products are just the beginning, however. Practices must still have someone either inside or outside the organization to tackle security issues. "A software program asks the right questions, but after a while people stop paying attention and say whatever they must to make the questions go away," says Lee. "Consultants will keep asking you the questions you need to answer."

"You need an expert," urges Futch. "It's a big job." His firm uses its own software and provides free evaluations, as well as staff interviews, to develop a plan for practices. "Then we identify risk and provide fixes." In his experience, backup issues reflect the most common shortcomings. "I've seen situations where people thought they had virus protection and complete backup, and it turns out they had neither."

Avoiding security breaches simply makes good sense. Take steps to become compliant now. "Things happen," Futch warns. "Something as simple as bad weather can lead to disaster."

*Reported and written by Deborah Epstein, contributing editor, in West Milford, NJ. For more information on HIPAA compliance, visit our Web site (see page 8).*

# MDCOMPLIANCE.com

Now Available Online!

Our **FREE** online resource includes:

**ENSURING APPROPRIATE REIMBURSEMENT**

Information focusing on how to code to ensure appropriate reimbursement while minimizing audit risk

**MINIMIZE AUDIT RISK**

Coding compliance strategies

**RESOURCE LINKS**

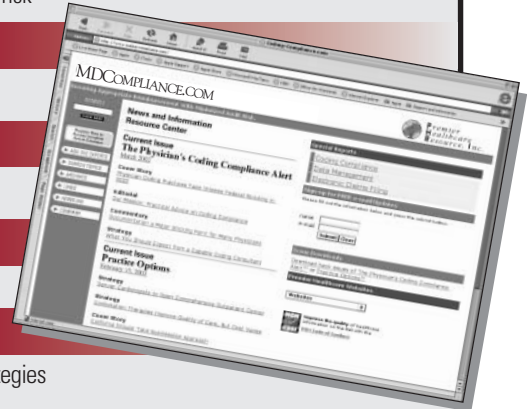
Links to coding compliance resources

**ASK OUR EXPERTS**

Coding compliance Q&A and interaction

**EMAIL UPDATES**

Email updates on the latest coding compliance strategies



Bookmark **www.MDCompliance.com** to your Internet favorites

May 2005

## THE PHYSICIAN'S COMPLIANCE ALERT™

PROVIDING PHYSICIANS WITH MEDICAL PRACTICE COMPLIANCE SOLUTIONS



Premier Healthcare Resource  
150 Washington St.  
Morristown, NJ 07960

PRSR STD  
U.S. POSTAGE  
PAID

Permit No 664  
S.Hackensack, NJ