

# THE PHYSICIAN'S COMPLIANCE ALERT™

PROVIDING PHYSICIANS WITH MEDICAL PRACTICE COMPLIANCE SOLUTIONS

## Is Your Practice Ready for the New HIPAA Privacy Rule?

**M**any practices are probably realizing about now that they are ill-prepared to meet the federal government's new patient information protection rule, which goes into effect April 14, 2003. But whether you're ready to roll or not, the Office for Civil Rights (OCR) at the US Department of Health and Human Services begins enforcement of the Healthcare Insurance Portability and Accountability Act (HIPAA) privacy rule next month.

Even if you have taken steps to meet compliance rules, it is important to know that the law requires more than buying a manual or giving a passing nod to patient privacy. The new regulations make broad changes in the way health care providers may use and disclose protected patient

information; those who fail to comply with the changes risk fines, exclusion from the Medicare program, and even prison terms. Violation of even minor provisions can result in civil fines of \$100 to \$25,000 per year. Intentional misuse of confidential health information can lead to criminal fines of \$50,000 to \$250,000 and sentences of one to 10 years in jail.

In addition to criminal penalties, civil suits against providers are likely to result from transgressions. Although the government will not actively seek out violators, the OCR will investigate any complaints, says Michael W. Carbrey, a health care consultant based in Celebration, Fla. These can come from patients or whistle-blowers in your practice. Especially worrisome are patient/personal-injury attorney complaints. Law firms may soon run advertisements that invite people to call if they think their privacy has been violated. To avoid these risks, practitioners must take specific actions—and make some changes in the way they think about protecting information.

### Legislators get HIPAA

Passed in 1996, HIPAA covers a lot of ground, including health insurance protection for workers, prevention of health care fraud and abuse, electronic submission of bills, and computer

security. Protection of patient information is also part of the act.

"Patient information used to be kept in the brain of Dr. Smith, but times have changed," says Carbrey. "That was before we had electronic transmission, personal digital assistants, and copies being requested by everyone for everything under the sun. It was also before patient information was leaked from a truck all over a highway," he continues. "Or entire patient files were found in landfills. Or the public learned that someone bought a retiring physician's charts and tried to sell them back to the doctor's patients." The HIPAA privacy rule was passed in the hope of preventing just such events.

No matter what the size of the medical practice, all providers who submit identifiable health information electronically (via magnetic tapes, computer disks or diskettes, compact discs, the Internet, or e-mail), including those who submit patient bills electronically, are "covered entities" under the regulations. These mandate the protection of information pertaining to the past, present, or future physical or mental health of an individual; the provision of health care for any individual; or the payment for health care for any individual, whether it can be found in standard medical records, personal

(Continued on page 6)

### CONTENTS

#### Editorial

Physicians Overwhelmed by Regulatory Activities .....2

#### Strategy

Feds Devoting More Attention to Coding Than in Prior Years ...3

#### Questions From Readers

How Will the Fee-Schedule Delay Affect Our Payments? .....5

## Physicians Overwhelmed by Regulatory Activities

Consider some of the issues currently facing physicians: coding compliance, implementation of components of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), an overall reduction in the Medicare Physician Fee Schedule (MPFS), modifications in Part B Medicare billing, and a profusion of coding changes. Bank on more rigorous appraisals from both the Office of Inspector General (OIG) for the US Department of Health and Human Services as well as from managed care companies. You should even expect your patients to more thoroughly assess the payment notices they receive from Medicare and private insurers—the recent spate of corporate scandals has sensitized the public to matters of business integrity, and physicians' practices will most certainly not be exempt from scrutiny.

Of immediate concern is the successful application of the privacy standards associated with HIPAA. These must be in effect for each medical practice by April 15, 2003. Our cover article discusses this most important area in greater detail. You can also learn more about the OIG's 2003 Work Plan, which details an array of potential risk areas for physicians; four of these involve proper coding. Note too, that the new MPFS went into effect on March 1, 2003.

Generally, you will be paid 4.4% less in 2003 than you received in 2002 for services provided to Medicare recipients. However, you should be paid at 2002 rates for care rendered in January and February of this year. An answer to a reader's question explains why this is so. In a future issue of the *Physician's Compliance Alert*, we will discuss ways to offset your financial loss. Ample documentation is an important way to protect your income. The federal government has successfully recouped millions of dollars from physicians who appeared to have been overpaid. More likely, these physicians had under-documented services rendered to patients and were thus unable to prove they had earned the fees they were forced to return.

During 2003, we intend to address numerous compliance areas, including the Clinical Laboratory Improvement Amendments, Occupational Safety and Health Administration requirements, and, of course, coding compliance. As always, we welcome your questions and comments and look forward to offering you meaningful information in the year to come.



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.

Jerry E. Block, MD  
Southeast Kansas Internal  
Medicine Associates  
Coffeyville, Kan.

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  
Deaconess Medical Group  
Evansville, Ind.

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  
Physician Management Group  
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)  
Web: [www.Coding-Compliance.com](http://www.Coding-Compliance.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.

# Feds Devoting More Attention to Coding Than in Prior Years

**I**n its General Work Plan for fiscal year 2003, the Office of the Inspector General (OIG) of the US Department of Health and Human Services (HHS) is targeting four major areas that relate to physician coding. One new project will investigate whether carriers are inadvertently paying physicians for claims that should have been rejected in accordance with Medicare's National Correct Coding Initiative. For example, are physicians billing for components of a procedure rather than using a single code that encompasses all of those individual steps?

Also new is the OIG's intention to examine claims for physician evaluation during dialysis. Specifically, investigators will be looking for evidence of up-coding. Are physicians billing as if a procedure required multiple evaluations when only a single assessment was required? Those procedures involving repeated evaluations are paid at a higher rate. The OIG will also revisit two coding areas first addressed in 2002: physicians' coding of evaluation and management (E&M) services and billing for consultations.

Six other items on the OIG's latest checklist pertain to physicians accepting Medicare. Claims for bone density screening will be investigated as will claims for long-distance physician encounters and billings for services and supplies incidental to physicians' services. The agency will also look into the relationship between optometrists and ophthalmologists sharing management of patients needing cataract surgery, financial arrangements between physicians and ambulatory surgical centers, and reassignment of benefits by emergency department physicians employed by staffing companies.

## Check your numbers

While the OIG plans to study each of these areas, "it doesn't mean there's

anything wrong," explains Judy Holtz, an OIG spokesperson. Some situations are routinely examined every year or two, and others may be studied at the request of the HHS secretary or the US Congress, she explains. Certainly, though, peculiarities—and big expenditures—do increase the likelihood of closer inspection. "If we see a spike in an area—say last year \$3 billion was paid out and then this year it was up to \$17 billion—that would raise a red flag, and we'd know we'd better take a look," Holtz notes, suggesting that physicians "look at this as a road map of what we plan to do." Closer examination of the OIG's guide indicates that studies of E&M coding, physician evaluation of dialysis coding, and long-distance claims will not actually be completed until fiscal year 2004.

But Charles E. Colitre, president of Med Management Group, Inc., based in Akron, Ohio, believes physicians should absolutely be concerned about the focus of the OIG's work plan. "The government feels these are problematic areas, so physicians will be under greater scrutiny and if not now, then soon," he says. "They should take a look at how they operate in these particular areas and see if they are doing things correctly." An area of particular concern, according to Colitre, is coding of E&M services.

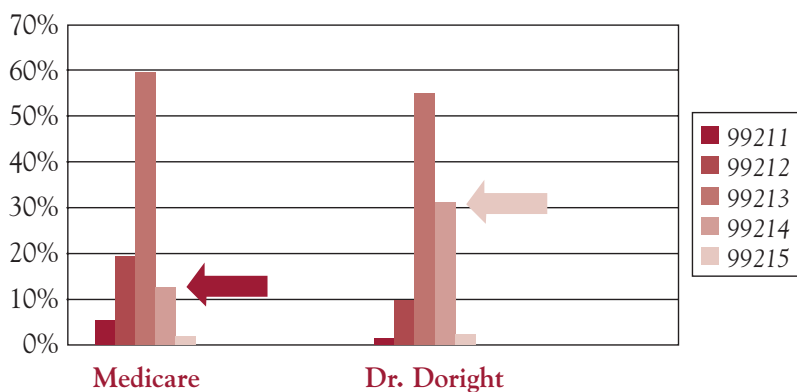
The OIG, which states that Medicare paid more than \$17 billion for E&M claims in 2001, plans to look into mechanisms used to identify physicians with aberrant coding patterns; that is, physicians who are costing the system more by "coding disproportionately high volumes of high-level" E&M codes.

The Centers for Medicare and Medicaid Services (CMS) determines patterns of E&M coding for physicians within specific geographic and specialty areas and uses these as a benchmark. For example, when the number of claims submitted by a general practitioner for new patient visits or established patient visits at each of the five levels of service are amassed and plotted on a graph, the points should ideally produce a bell-shaped curve, with the majority of patients being billed at level three and the minority of patients being billed at level one or level five, Colitre says. If the physician bills a majority of claims for new patient visits at level four, he indicates that a closer look is warranted to determine the legitimacy of the coding pattern (see figure, page 4).

"It's not that a physician is necessarily over-coding," says John McDaniel, president and CEO of Physician Management Group, Inc., headquartered in New Orleans, La. "He may just have an unusually high

*(Continued on page 4)*

## Comparison



Source: Med-Management Group, Inc. ©2002

(Continued from page 3)

number of sick patients. But hopefully, if he is audited, his documentation will support what he has charged.” A seemingly out-of-bounds billing pattern might be normal for physicians who consistently take care of very ill patients—critical care specialists, for example. Still, the CMS compiles national usage distributions for a variety of specialties, and coding outside peer averages will often lead to an audit, Colitre points out. Relatively small statistical samples of a physician’s charts are checked to compare documentation with coding. Where the coding and documentation do not match, the claims are down-coded by the carrier, or in some cases, completely disallowed. The physician is then directed to reimburse the CMS.

If the carrier believes the discrepancy is the result of fraud or if a physician continues to bill outside the peer averages, the matter will be referred for further investigation. Colitre says that physicians who find themselves in this position might have to pay severe penalties. A fine may be tallied at three times the overpayment amount, plus civil monetary penalties of \$5,500 to \$11,000 per claim. Even a small number of claims can turn into a “multimillion dollar exposure,” he warns.

### Protect yourself

Some physicians bill at a higher level in order to earn enough to keep their practices open, Colitre remarks. Others bill at a lower rate because they fear being audited. “So then you have two situations—one where they’re over-billing and over-coding, which is illegal, and one where they’re under-coding and under-billing, which means they’re leaving money on the table that they could rightly be collecting,” he adds. To avoid either extreme, Colitre recommends that physicians conduct regular audits of coding patterns to determine whether they are out of line with other physicians in their practice as well as other physicians in the country.

“I always recommend they bring in an outside person to do that audit,” Colitre urges. “Then, if they’re doing well, they might be able to continue that process internally. But my recommendation, and the recommendation of most people in this business, is that once a year, it’s good to get a coding checkup from outside.”

Your best defense is to carefully record what occurs at each patient visit to support the level of care for which you ultimately charge. “The

E&M codes have some pretty complex components that the physicians have to document correctly,” Colitre says. To help steer your efforts, you can rely on either of two versions of the Documentation Guidelines for Evaluation and Management Services distributed by the CMS. The 1995 set is “more flexible,” he observes.

McDaniel says consultation coding is another area that typically confounds physicians. The OIG will study the appropriateness of billings for physician consultation services and the tab resulting from payment of inaccurate claims. “Consults pay more than a new patient visit,” he comments. “So what Medicare is concerned about is whether a true consultation has occurred or whether the second physician is continuing the care.” When the physician assumes care without providing feedback to the original caregiver, the encounter is actually a referral. “That’s a very fine line,” McDaniel emphasizes.

The OIG states that in 2000, the CMS paid out \$2 billion for consultations. “Let’s just assume that 10 percent of those were not consults,” McDaniel adds. “That’s \$200 million, which is not an insignificant amount of money.”

Despite its plans to check over physicians’ billing activities, the OIG believes that most physicians are correctly billing Medicare for their services, Holtz says. “The vast majority of members of the provider community are honest and doing the right thing,” she concludes. “There are a few bad apples in the industry, so we all just need to work together to rid the program of its problems in order for it to run smoothly for everyone else involved.”

Reported and written by Theresa Waldron, in Marietta, Ga. More information on the OIG and documentation is available on our Web site ([www.Coding-Compliance.com](http://www.Coding-Compliance.com)).

# How Will the Fee-Schedule Delay Affect Our Payments?

**Q:** Should providers be submitting the new CPT codes for 2003 despite delayed publication of the Medicare Physician Fee Schedule (MPFS)? Would it be a compliance issue if we continued billing with the old codes because they guarantee payment? What if a new 2003 code more appropriately describes the service?

**A:** In any circumstance where no appropriate CPT code exists for a particular service, you should use an unlisted code, advises Rhonda Lynn Picou, RN, MSN, CPC, vice president of physician compliance for Physician Management Group, Inc., headquartered in New Orleans, La. Otherwise, the final rule outlining the MPFS was published on December 31, 2002, and the new rates described within became effective on March 1, 2003. As a result, use of the new 2003 MPFS HCPCS codes would have been best postponed until you began billing for services provided on or after that date, Picou says. If you already used the 2003 codes on claims for services rendered in January and February of this year, you probably found those claims were stalled in the carrier's system until at least March 1. After processing, they were and will be paid at the 2003 rate. Physicians submitting "clean" claims may be entitled to interest.

Ideally, claims resulting from services provided in January and February should have been prepared with 2002 codes. Those processed by February 28, 2003, were paid at the 2002 rate. Claims handled at a later date are initially being paid at the 2003 value. However, you will receive an additional increment later in the

year—as of July, carriers will be able to make automatic adjustments in payment for services that were provided patients in the first two months of the year and billed with 2002 codes. You do not need to contact your carrier in order to receive the extra amount. The Centers for Medicare & Medicaid Services (CMS) notes that you do "not need to take further action to receive the adjustment payments."

Payments for services not included in the MPFS have been and will be paid at 2003 rates, a system that began on January 1, 2003. As you probably know, the 2003 rates are 4.4% lower than those rates paid for services provided in 2002. The reduction stems from a defect in the formula used to determine the fee schedule, according to the CMS. While the agency hopes to correct the flaw to prevent further fee reductions in the future, the calculation is part of Medicare law and Congress must approve any alteration. The CMS says that it plans to continue working with Congress toward "changes that could have a positive impact on physician payments."

**Q:** A patient came in with gangrene of the toe. We called a podiatrist who has an office in our building and requested a consultation with him. After he had examined her, we treated the woman for uncontrolled diabetes, hypertension, and congestive heart failure during the same visit. How can we code so that we're paid for both the office visit and the consult?

**A:** You cannot charge for the consultation. Instead, the

podiatrist can bill Medicare for his services and you can bill for the rest of the care given, Picou says. Even though two practitioners attended to the same patient during the same visit, each provided distinctly different services. To best ensure that you and your colleague are paid appropriately, you should document the request for the consultation, and the podiatrist should document what transpired during his evaluation of the patient's gangrenous toe. The information should then be retained in the podiatrist's records. You should also receive a copy of this report so that it can be attached to the patient's chart for further reference.

**Q:** How should a physician code evaluation and management (E&M) services when these are provided at the assisted living facility in which the patient lives? Would the visit be considered a home service or a domiciliary service?

**A:** Use the E&M codes for domiciliary, rest home, or custodial care services, Picou urges. This category pertains to facilities, including those for assisted living, where people can reside on a long-term basis, receiving meals and assistance with daily tasks. However, these establishments do not provide medical care. Specifically, codes 99321 to 99323 are used for visits to new patients; 99331 to 99333 are employed for visits to established patients.

*Editor's note: Readers of The Physician's Compliance Alert are invited to visit our Web site at [www.Coding-Compliance.com](http://www.Coding-Compliance.com) and submit their questions. Members of our Advisory Board will offer their expert opinions on a variety of situations.*

notes, or claims, observes Carbrey.

### **What you need to do**

HIPAA is more than 900 pages long, and the amendments take up another 300 pages. As if that isn't overwhelming enough, many myths are circulating on what must be done to comply with the new law. The job is not as onerous as one might think, however. There are basically six actions that promote compliance.

First, provide written notices of your privacy practices to patients. These will also tell patients what the privacy regulations are. This is required by law and must be done at the first office visit after April 14, 2003. Develop appropriate technical and physical guidelines to protect the privacy of shielded health information and reasonably safeguard such information from intentional and unintentional use or disclosure.

Train employees on privacy guidelines and on what the privacy law requires. This includes all new personnel as well as volunteers and any other individuals who work in the practice. Training should include: awareness training for all personnel, including management; periodic security reminders; education on computer virus protection; emphasis on the importance of monitoring log-ins, and methods of reporting possible problems; and user education in managing computer passwords.

Designate a privacy officer who will be responsible for the use of security measures and the conduct of personnel in relation to the protection of data. This function need not be full-time, and the privacy officer can delegate specific tasks to others.

Establish a system to account for all private health information disclosures. As of April 15, patients will have the right to ask providers how many times their health information

has been disclosed and to whom. The exception to this rule is data sent for the treatment of the patient, such as that sent to medical insurance companies for billing purposes and to pharmacists or other physicians who are involved in the patient's care. Information sent to life insurance companies, data on clinical studies, and information for grants are covered, however. Patients can request all disclosures dating back six years from the date of the request.

Form contracts to ensure privacy of information with all "business associates" who may or may not have access to protected health information. This includes, for example, those who perform claims processing, utilization review, quality assurance, consulting, practice management, or legal counseling. Such "chain of trust partner agreements" are required for all third-party data processors with whom the organization contracts. They state that all parties agree to electronically transmit data and to protect the transmitted data. Those with contracts made prior to October 15, 2002, have until April 15, 2004, to complete new contracts. If contracts were made after October 15, 2002, they should be completed before April 14, 2003. If existing contracts expire after October 15, 2002, new contracts must include business associate agreements. This step is the only one that requires the services of an attorney to review the contracts. Aside from these legal fees, practices can generally accomplish all six steps for less than \$500, with formalized training accounting for about \$50 per employee.

### **Managing security**

Although specific policies and procedures are not spelled out in the privacy rule, they should certainly include several important components to be effective. One necessary element is a

process for conducting on-going audits, which allow you to review electronic systems activity. This means developing a way to conduct periodic reviews of log-ins, film access, and records of security-related incidents. Also needed are guidelines for security management as well as reporting and responding to breaches of security. This includes the areas of risk analysis and management, sanctions, containment of security breaches, and identification and reporting of such breaches.

Contingency plans for system emergencies must also be in place to help preserve security. To deal with system emergencies, practices should have a data backup plan, a disaster recovery setup, plans for an emergency mode of operation, and written policies and procedures for testing and revising the system.

### **Software assistance**

For those practices that are not in compliance with the privacy rule at this late date, the best choice is probably the use of a software product that guides the user through the compliance process step by step. Such products can also be of use to practices that still need certain forms or training tools to help them comply.

Medical Data Applications Ltd. (MDA), located in Jenkintown, Pa., offers an especially comprehensive and reasonably priced software product, according to Carbrey. The company markets HIPAAzip, which consists of a compact disc, a manual, and searchable versions of HIPAA. Also included are all the forms and documents required by the privacy rule, including forms for disclosure authorizations, notices of privacy practices for patients, denials of access notifications, and denials of amendments. "HIPAAzip is particularly suited to the needs of independent

*(Continued on page 7)*

practices,” says Libby A. Hudson, vice president of marketing and sales for MDA. “Most of the health care practitioners that are covered under HIPAA have limited technical knowledge about computers. Our goal was to ensure that the program will install and work correctly out of the box on virtually any vintage of computer or Windows operating system.”

The software also includes educational materials, such as a slide show and tests, for staff training. Forms in English and Spanish can be customized; a business associate agreement, written by a health care attorney, is included as well. “The burden of attempting to achieve compliance on their own is likely to be overwhelming for most small to medium-sized health care practices,” says Richard H. Epstein, MD, president of MDA. “HIPAAzip organizes the compliance and training process in a simple, straightforward manner,” he adds. HIPAAzip has been endorsed by the IPA Association of America, and members of that organization can purchase the product through the association’s Web site (at [www.TIPAAA.org](http://www.TIPAAA.org)). Non-members can purchase the product at the MDA Web site ([www.MDA-Ltd.com](http://www.MDA-Ltd.com)). The cost of HIPAAzip is \$395.00.

### **Correcting false impressions**

Some myths need to be dispelled concerning what’s required by HIPAA, according to Carbrey. For example:

- **Practices cannot use fax machines.** You can use faxes to send protected health information, but you must ensure that all information reaches the correct destination and that the recipient’s fax machine is not open to the public.
- **Practices need to soundproof offices.** Offices do not need to be made soundproof, but be aware that

## **Software Security**

The government has not yet released standardized electronic data sets, which will tell providers how to send electronic billing data and delineate who can receive the data. Meanwhile, however, health information that is stored electronically is protected by the privacy act. Keeping software and electronic data secure is therefore critical. Listed here are steps you can take to help ensure that your data is secure:

- When data are copied to disks or other media, ensure that you store the disks in a secure location.
- Protect computer information with passwords. These should be changed once a month as well as any time an employee leaves the company. Termination procedures should also include changing combination locks, removing terminated employees from access lists and user accounts, and retrieving keys or cards that allow access to any protected information.
- Limit computer access to those employees who require it in order to do their jobs. In addition, each employee should only be able to get into the data pertinent to his or her specific tasks.
- If you use an off-site computer to process or forward information, make sure you use a secure line with the necessary firewalls. Also limit access for others who use the server on a need-to-know basis.
- Have policies and procedures in place to ensure that routine changes to hardware or software do not create security weaknesses. This includes measures to be used in testing of new hardware and software for security features, routine security testing, checking for computer viruses, and in taking inventory of hardware and software.
- Finally, be certain that all system users are trained in system security.

people might be able to hear conversations. Keep doors closed and speak low when patient information is being discussed.

- **Practices must put locks on all filing cabinets.** Filing cabinets do not have to be locked, but records should be secured from those who are not allowed access to protected health information.
- **Sign-in sheets can no longer be used.** Sign-in sheets may be used, but they should not include patient diagnoses or complaints.
- **Files cannot be placed in racks outside the door.** Not so. Files may be placed in a rack outside the door.
- **I can’t say a patient’s name in public.** This is not true. Providers and staff can acknowledge patients

by name in public. For instance, saying, “Hello, Mr. Smith” in the waiting room or hallways is fine. Conversations should not include diagnostic or other health information. For example, saying, “Hello, Mr. Smith. How is the Viagra working?” is certainly a violation.

In other words, use common sense when it comes to patient information. This generally comes down to protecting conversations and files—and teaching staff members one important rule: what they hear and see inside the practice must stay inside the practice.

*Reported and written by Deborah Epstein, in West Milford, NJ. More information on HIPAA is available on our Web site (at [www.Coding-Compliance.com](http://www.Coding-Compliance.com)).*

# CODING-COMPLIANCE.com

Now Available Online!

Our **FREE** online resource includes:

#### MAXIMIZING REVENUE

Information focusing on how to appropriately code to maximize practice revenue 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.Coding-Compliance.com](http://www.Coding-Compliance.com) to your Internet favorites



March 2003

## 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 1354  
S.Hackensack, NJ