

# Regulatory Issues Present Burdens for Practices

**P**hysicians who participate in Medicare and Medicaid know the government's rules and regulations for these programs are burdensome, and enforcement is more aggressive than ever.

The U.S. Department of Health and Human Services (HHS) says that most Medicare payment errors are simple mistakes and

**The Department of Health and Human Services** says that most Medicare payment errors are simple mistakes and are not the result of physicians, providers or suppliers who are trying to take advantage of the programs. HHS maintains, however, that there are a few individuals who are intent on defrauding Medicare out of millions of dollars annually.

are not the result of physicians, providers or suppliers who are trying to take advantage of the programs. The vast majority of physicians serving Medicare and Medicaid beneficiaries are committed to providing high-quality care to their patients and to billing the program only for payments they have earned.

It is also important to remember that physicians are not subject to civil or criminal penalties for innocent errors or even negligence with

regard to the Medicare and Medicaid programs. Erroneous claims result only in the return of funds claimed in error.

HHS maintains, however, that there are a few individuals who are intent on abusing or defrauding Medicare and cheating the program out of millions of dollars annually. As a result, the Centers for Medicare & Medicaid Services (CMS) is taking strong action to combat fraud and abuse of the system in key areas.

CMS Administrator Mark B. McClellan, M.D., Ph.D., recently said that several areas of the country have been identified as fraud "hot spots." To help combat fraud and abuse problems in one of these geographic areas, CMS opened a satellite office in South-

ern California to focus on the large number of reported fraudulent activities occurring in that part of the country. The activities include illegal storefront operations set up to bill for services never provided to beneficiaries.

In addition, CMS announced that it is using a data-oriented approach to uncover fraud and abuse. It expanded the Medicare-Medicaid match program, in which claims data from both programs are analyzed together to detect patterns that may not be evident when billings for either program are viewed in isolation. As a result, it can identify undetected patterns such as “time bandits,” providers who bill for a total of more than 24 hours in a day in both programs.

### **Enforcement Actions**

The Office of Inspector General (OIG) investigates Medicare and Medicaid fraud and takes action if it uncovers unlawful activities. The Civil Monetary Penalties Law authorizes the OIG to impose administrative penalties and assessments against a person or entity that submits to a federal healthcare program claims that the person should know are false or fraudulent.

The OIG says that one of the most common types of fraud perpetrated against Medicare and Medicaid involves the filing of false claims for reimbursement. The OIG is able to pursue false claims under the civil False Claims Act and, in appropriate cases, under federal and state criminal statutes. The OIG has the responsibility to assist the Department of Justice in bringing and settling cases under the civil False Claims Act.

Many of the providers investigated by OIG enter into settlements that include cash penalties and integrity agreements that allow them to continue to participate in government healthcare programs. These agreements are monitored by OIG and require the providers to establish new or to enhance existing compliance programs. The compliance programs are designed, in part, to prevent a recurrence of the underlying fraudulent activities.

In the six months ending March 31, 2005, the federal government negotiated \$1 billion in civil and administrative settlements related to Medicare, Medicaid and other federal healthcare programs, according to the OIG's 2005 semiannual report.

Much of that amount was recouped from large healthcare

providers such as hospitals, clinics, durable medical equipment suppliers, home health agencies and pharmacy chains. One example involving a physician cited in the semiannual report is the case of a Florida radiology group that was fined \$2.5 million for allegedly submitting false claims to Medicare over a six-year period. The claims involved allegedly billing for services that were not ordered by the treating physicians, upcoding of claims, and unbundling of services billed.

During this reporting period, OIG also administered 1,702 sanctions in the form of program exclusions or administrative actions for alleged fraud or abuse or other activities that posed a risk to Federal healthcare programs and their beneficiaries.

If you haven't already done so, it is important to establish a

### **Billing Practices Subject to Scrutiny**

The following risk areas associated with billing have been among the most frequent subjects of investigations and audits by the Office of Inspector General:

- Billing for items or services not rendered or not provided as claimed.
- Submitting claims for equipment, medical supplies and services that are not reasonable and necessary, based on the patient's documented medical condition.
- Double billing resulting in duplicate payment.
- Billing for non-covered services as if covered.
- Knowing misuse of provider identification numbers, which results in improper billing. An example of this is when the practice bills for a service performed by Dr. B, who has not yet been issued a Medicare provider number, using Dr. A's Medicare provider number.
- Unbundling, or billing for each component of the service instead of using an all-inclusive code. For example, if dressings and instruments are included in a fee for a minor procedure, the provider may not also bill separately for the dressings and instruments.
- Failure to properly use coding modifiers.
- Clustering, which is the practice of coding/charging one or two middle levels of service codes exclusively, under the philosophy that some will be higher, some lower, and the charges will average out over an extended period.
- Upcoding the level of service provided, or billing for a more expensive service than the one actually performed.

comprehensive compliance program so you can stay on the right side of federal health programs including Medicare, Medicaid, the Stark regulations on self-referrals and the Health Insurance Portability and Accountability Act (HIPAA).

A compliance program is designed to help you use internal controls to monitor adherence to federal healthcare statutes, regulations and program requirements. The OIG points out that a good compliance program not only helps prevent fraudulent or erroneous claims, but may also show that your practice is making a good-faith effort to submit claims appropriately.

**An effective compliance program** should address the types of fraud and abuse-related topics that are most likely to confront your practice. The HHS Office of Inspector General has developed a list of potential risk areas affecting physicians. These include coding and billing; reasonable and necessary services; documentation, and improper inducements, kickbacks and self-referrals.

This program should consist of policies and procedures designed to detect, prevent and correct violations of healthcare laws. It can be modeled after the OIG's guidelines for such programs. (View the

guidelines at [www.oig.hhs.gov/authorities/docs/physician.pdf](http://www.oig.hhs.gov/authorities/docs/physician.pdf)).

The OIG says that you should determine the types of fraud and abuse related topics to address based on your specific needs. It has developed a list of potential risk areas affecting physicians. These include coding and billing; reasonable and necessary services; documentation, and improper inducements, kickbacks and self-referrals.

In addition, the government says that one of the most common risk areas involving billing services deals with physician practices contracting with billing services on a percentage basis. The OIG has a longstanding concern that such arrangements may increase the risk of intentional upcoding and similar abusive billing practices.

In addition, an effective compliance program should include a clear policy on how to respond to government inquiries, says Neil B. Caesar, Esq., president of the Health Law Center, a national health law firm headquartered in Greenville, S.C. Although the government provides guidance in this area, the assistance of legal

counsel may be necessary when establishing your compliance plan because you may want the benefit of attorney-client privilege.

“Efforts to stay within the confines of the attorney-client privilege will enable a medical group to establish a compliance plan more quickly and less expensively than would otherwise be possible,” Mr. Caesar maintains.

With the attorney-client privilege, if the government were to ask for a patient’s medical records to identify whether the provider had appropriately documented the care provided, the provider could not hide behind attorney-client privilege to prevent turning over the records, he explains. But if the provider had already discussed the problem of poor documentation and what to do about the government’s inquiry with the lawyer, those discussions could be protected.

## Elements of Compliance

The OIG compliance model includes seven elements that are fundamental to an effective program:

- Establishing compliance standards through a code of conduct and implementing written policies. The code of conduct should include the practice’s expectations with respect to billing and coding, patient care, documentation and payer relationships.
- Designating a compliance officer or contact in your office. This individual can oversee and monitor the implementation of the compliance program and establish methods, such as periodic audits, to improve the practice’s efficiency and quality of services and reduce the practice’s vulnerability to fraud and abuse.
- Conducting comprehensive training on practice ethics and policies and procedures, and focusing on areas such as correct coding, billing and documentation. The training component includes determining who needs training in coding, billing and compliance, and deciding the type of training that is best for the practice, such as seminars, self-study or other programs.
- Conducting internal monitoring and auditing, focusing on high-risk billing and coding issues through performance and periodic audits.
- Enforcing standards through well-publicized disciplinary guidelines and making sure that compliance is treated seriously and that violations will be dealt with consistently and uniformly.

■ Responding promptly to detected offenses and undertaking corrective action. It is important to have procedures in place to enforce and discipline individuals who violate the compliance program or other standards. The government believes that enforcement and disciplinary provisions are necessary to add credibility and integrity to any compliance plan. Disciplinary actions may include oral warnings, written reprimands, probation, demotion, suspension, termination and even a referral for criminal prosecution.

■ Developing open lines of communications so it is possible to have frank discussions if problems do occur.

In a small practice, you should establish a clear open-door policy between the physicians and the compliance individual. This can include a requirement that employees report conduct that a reasonable person would believe to be erroneous or fraudulent. An anonymous drop box could be used in larger practices to report this conduct.

Experts say that several months after you've set up your compliance program, you should conduct a baseline audit of your practice and continue with annual audits afterwards. You may wish to use a law firm and practice management consultant to review your current practices on billing, referrals and vendor relationships to make sure they are compliant with the law. If problems are discovered during the audit, it is important to address them within 60 days after they are discovered.

### **Errors Often Honest Mistakes**

Confusion over Medicare rules often cause well-meaning physicians to make honest mistakes. Small medical practices in particular find it extremely difficult to stay on top of an ever-changing situation. Most of these practices lack the money to hire risk managers, accountants and attorneys to help in this area.

Medicare coding and billing errors, for example, continue to be a problem for many practices. According to the Centers for Medicare and Medicaid Services (CMS), of the total payments sampled in 2004, 4.1 percent had errors due to insufficient documentation being submitted, and 2.8 percent had errors due to non-responses to requests for medical records.

## When the Government Visits

Above all, be sure you are prepared if the federal government decides to pay you an office visit, says Mr. Caesar. It is a good idea to write down your policies on government investigations as part of your compliance plan.

These policies should deal with document requests, on-site inspections, interviews and search warrants. In addition, each of your employees should understand what is expected of him or her during an investigation.

When officials come to your office, Mr. Caesar recommends asking to see identification from the person in charge of those conducting an inspection or executing a search warrant. Be sure to record the name, location, agency and title of the individual. If the government officials produce a search warrant, you should contact your attorney immediately. Mr. Caesar recommends having your attorney's number on your speed dial.

Be sure to select an attorney who understands health law issues and government investigations. But be advised that it is likely that the federal officials will probably begin the investigation immediately and not provide time for your attorney to get to the phone or arrive at your offices.

In addition, it is important to designate one person on your staff (it may be you) who is responsible for watching everything taking place during an investigation. Whoever has this responsibility in your office should introduce herself or himself to the federal official and request that all questions or comments from the official be directed to the staff person in charge of investigations.

Your staff should not interfere with the investigation in any way. They should speak truthfully and not speculate about past events. Further, Mr. Caesar says that it is dangerous to tell your employees not to talk to the officials or to encourage them to take that stance; the government may consider such actions to be evi-

**When government officials come to your office, attorney Neil Caesar recommends asking to see identification from the person in charge of those conducting an inspection or executing a search warrant. Be sure to record the name, location, agency and title of the individual. If the government officials produce a search warrant, you should contact your attorney immediately.**

dence of “obstruction of justice.”

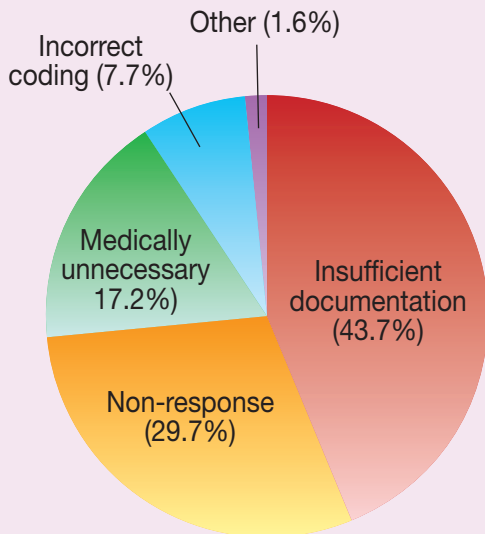
Your staff should know, however, that they do not have to talk with the government agents at the time of their investigation. They have the right to have an attorney and/or representative of your organization present when they are being questioned.

Also keep in mind that search warrants frequently give federal officials the right to take computer software and hardware, and not just printed information. In some cases, the officials may be content with a download of your computer’s information.

Mr. Caesar says that, at a minimum, you should try to create a backup of your hard drive before the government removes your computers. It is wise to make backups routinely so that you can retrieve any seized information. Further, get a detailed receipt for

### Medicare Errors by Type

Percentage of the total number of errors in fiscal 2004



Source: Centers for Medicare and Medicaid Services.

all the material that the officials take. Before you sign the receipt, make certain that it is complete and accurate.

## Handling Overpayments

Overpayments are considered by CMS to be Medicare funds that a provider or beneficiary has received in excess of amounts due and payable under the statute and regulations. Once a determination of overpayment has been made, the amount determined to be an overpayment is a debt owed to the federal government. Federal law requires CMS to seek recovery of overpayments, regardless of how an overpayment may be identified or caused.

**Overpayments** are considered by CMS to be Medicare funds that a provider or beneficiary has received in excess of amounts due and payable under the statute and regulations. Once a determination of overpayment has been made, the amount determined to be an overpayment is a debt owed to the federal government.

Overpayments can take place for a number of reasons, including a duplicate submission made for the same service or claim, and payment made to the wrong provider.

CMS says that if Medicare pays more than the correct amount in error, providers are responsible for making voluntary refunds to Medicare as soon as possible, without waiting for notification.

Contact your local Medicare carrier to find out where to mail the refund. When sending in a refund, CMS says it is important to include the following information:

- The provider number (and that of the provider who should have been paid, if applicable).
- The Medicare number of the patient(s) in question, date of service and amount overpaid.
- A brief description of the reason for the refund.
- A copy of the remittance notice, highlighting the claim(s) that are at issue.
- A check for the overpaid amount.

If Medicare discovers an overpayment before a physician makes a refund payment, providers and suppliers are also responsible for timely repayment when they receive a notice from CMS about the overpayment. Physicians can expect to receive a letter

listing the service(s) at issue, why the overpayment occurred and the amount being requested. If the overpayment is not paid in full in 30 days, interest will start accruing on day 31.

Be sure to heed the request from Medicare because if you don't, you will receive a second demand letter from the agency. If full payment is not received 40 days after the date of the first demand letter, the Medicare carrier will begin recouping the overpayment from future payments on day 41. If physicians fail to make reimbursements in full, they could be hit with civil monetary penalties and exclusion from Medicare participation.

If you disagree with the overpayment assessment, you have the right to appeal the decision. According to CMS, recoupment by Medicare will stop if the first recoupment action took place after Dec. 8, 2003, and the first-level appeal has been received.

To contact the Medicare contractor's toll-free customer service number in your area, go to the following Website: [www.cms.hhs.gov/medlearn/tollnums.asp](http://www.cms.hhs.gov/medlearn/tollnums.asp).

## Medicare Appeals Process

The federal government has a five-level appeals process for Medicare Part B providers. If you are a physician who does not participate in Medicare and accept assignment, CMS says you have limited appeal rights.

The first level of appeal is called redetermination; it is an examination of a claim by insurance carrier personnel who are independent of the personnel who made the initial determination. You have 120 days from the date of receipt of the initial claim determination to file an appeal.

You can request a redetermination in writing or by telephone. You can complete your written request by submitting Form CMS-20027, available at the following Website: [www.cms.hhs.gov/forms](http://www.cms.hhs.gov/forms). When requesting a redetermination by phone, be sure to have the information ready for filing a written request plus the beneficiary's date of birth.

Following redetermination, the next level of appeal is a hearing before a hearing officer. This can be an in-person hearing, at which you are allowed to present oral testimony and written evidence supporting the claim and challenging the information the carrier used to deny the claim. In addition, CMS allows telephone

hearings. These are a convenient and less-costly alternative to in-person hearings. Oral testimony and oral challenges may be conducted, and other evidence may be submitted by mail or fax.

The next level is a hearing before an administrative law judge. Physician claims cases rarely go beyond this level, according to an article by Kent Moore, manager of healthcare financing and delivery systems for the American Academy of Family Physicians, in an article in *Family Practice Management* (April 2003). But the mechanism exists to bring such cases before a Federal District Court.

CMS points out that Medicare contractors can't correct minor

### The Medicare Part B Fee-for-Service Appeals Process

APPEAL LEVEL	TIME LIMIT FOR FILING REQUEST	MONETARY THRESHOLD TO BE MET
1. Redetermination	120 days from date of notice of the initial determination	None
2. Hearing Officer (HO) hearing	6 months from date of redetermination	At least \$100 remains in controversy
3. Administrative Law Judge (ALJ) Hearing	Filed within 60 days of receipt of hearing decision	At least \$100 remains in controversy
4. Departmental Appeals Board (DAB) Review	Filed within 60 days of receipt of ALJ hearing decision/ dismissal	None
5. Federal Court Review	Filed within 60 days of receipt of DAB decision or declination of review by DAB	At least \$1,050 remains in controversy

Source: Centers for Medicare & Medicaid Services, *The Medicare Claims Processing Manual*.

errors and omissions on claims through the appeals process. The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) has set up a process for physicians to correct minor errors and omissions in claims without pursuing the formal appeals process. For information on how to correct minor errors, check out a CMS article at [www.cms.hhs.gov/medlearn/matters/mmarticles/2004/SE0420.pdf](http://www.cms.hhs.gov/medlearn/matters/mmarticles/2004/SE0420.pdf).

## Complying with Self-Referral Rules

In 2004, the CMS finalized what it considers to be clearer regulations on the federal self-referral law known as Stark so that physicians have a better idea of how to comply with this complex statute.

The Stark law prohibits physicians from referring Medicare and Medicaid patients to establishments and entities in which they or immediate family members have a financial interest unless the financial relationship fits into an exception under the

## Program Offers Medicare Information

Medicare is a vast and complex program, with ever-changing rules that make participation an administrative nightmare for many physicians. Making matters worse is that even the carriers that contract with Medicare to process claims often give erroneous information to physicians seeking information. A 2004 Government Accountability Office (GAO) report found that roughly 96 percent of telephone inquiries on Medicare billing policy to carrier call centers received incomplete or inaccurate responses.

The Centers for Medicare & Medicaid Services is trying to get accurate information to program participants through a service called the Medicare Learning Network. It is a multimedia educational program for Medicare providers of all types.

The Medicare Learning Network uses a variety of mechanisms, such as the Internet, "Medlearn Matters...Information for Providers" national education articles, brochures, fact sheets, Web-based training courses and videos, to deliver a planned and coordinated provider education program, says CMS.

For more information on the Medicare Learning Network, log on to [www.cms.hhs.gov/medlearn/](http://www.cms.hhs.gov/medlearn/).

law. The law also prohibits an entity from billing for services provided as a result of a prohibited referral.

The Stark statute is not the same as the anti-kickback law, which precludes payments in exchange for referrals of program-related items or services.

The anti-kickback statute is broader than Stark and affects anyone engaging in business with a federal healthcare program. Nevertheless, in every situation where the Stark statute applies, the anti-kickback statute applies too, writes Alice G. Gosfield, J.D., in an article published in the February 2004 issue of Family Practice Management.

The latest regulations, known as Stark II, are based on responses to comments CMS received on the first phase of Stark, and they create several new regulatory exceptions for “nonabusive” financial relationships. Many of these exceptions require that whatever financial relationships exist reflect fair market value.

Stark II established referrals for physician services within the group exception. Referrals from one physician to another for physician services must be provided either personally by or under the personal supervision of another physician in the same group practice.

Stark II defines “group practice” as a practice with two or more physicians who are legally organized and in which each member of the group provides substantially his or her normal full range of designated health services and other services in the group practice through the joint use of shared office space, facilities, equipment and personnel. In addition, members are not compensated based on volume or value of referrals, and group members conduct 75 percent of all patient encounters.

To be sure that you are not violating the Stark law, you should evaluate any economic benefits you receive from entities to which you refer Medicare and Medicaid patients in order to

**The Stark law** prohibits physicians from referring Medicare and Medicaid patients to establishments and entities in which they or immediate family members have a financial interest unless the financial relationship fits into an exception under the law. The law also prohibits an entity from billing for services provided as a result of a prohibited referral.

determine whether they meet any of the exceptions in the statute, Ms. Gosfield writes.

The Stark law is enforced by the HHS Office of Inspector General. Noncompliance carries substantial civil penalties. Direct sanctions under the law include a prohibition on billing, denial of payment and required refunds. Violations can also result in

**The Stark law is enforced by the HHS Office of Inspector General. Noncompliance carries substantial civil penalties. Direct sanctions under the law include a prohibition on billing, denial of payment and required refunds. Violations can also result in fines up to \$15,000 per claim, civil monetary penalties and potential False Claims Act liability.**

fines up to \$15,000 per claim, civil monetary penalties and potential False Claims Act liability.

The Stark rules define a financial relationship as either an ownership interest or a compensation arrangement, which can be either direct or indirect. Ownership interests include equity, secured loans, partnership shares, limited liability company memberships, stock options, bonds and other financial instruments.

There are 11 designated health services to which the prohibition applies, including radiation therapy; prosthetics, orthotics and prosthetic devices and supplies, and inpatient and outpatient hospital services. The new regulations interpret some exceptions for compensation arrangements involving physicians. For example, CMS eliminated a proposed restriction on productivity bonuses, making it clear that physician employees may be paid bonuses based on their personal productivity, but not for referrals for ancillary services.

Under Phase II, the rules governing when groups can share equipment, space and personnel for designated health services are more restrictive. To meet the exception, the services have to be in the same building. To satisfy the same building requirement, your office must meet one of three tests:

- Under the first test, the office is open to patients 35 hours per week, and the referring physician or group members regularly practice at the location at least 30 hours per week.

- Under the second test, the office is open to patients at least eight hours per week, and the referring physician furnishes services at the location at least six hours per week.

■ Under the third test, the office is open to patients eight hours per week, and the referring physician or group member furnishes services at the location for at least six hours per week. Further, the referring physician must be present and must order the designated health services in connection with the patient visit, or the group member must be present while the designated health service is furnished.

Stark II also creates a professional courtesy exception that allows doctors to provide free or discounted care to other physicians or their families. To qualify for this exception, a medical practice must meet six conditions. These include making sure the healthcare items and services provided are the type routinely provided and that the professional courtesy policy is set out in writing and approved in advance by the practice.

The regulations also modify physician recruitment and retention policies. For example, they focus on relocation of the recruited physician's medical practice, rather than his or her residence, and eliminate the relocation requirement for residents and physicians who have been in medical practice less than one year.

Because of the complexity of this law, legal experts recommend that you understand the factors that may implicate the statute and obtain legal advice when there are financial relationships associated with designated health services provided to Medicare and Medicaid patients.

## **HIPAA: Security and Privacy**

The Health Insurance Portability and Accountability Act (HIPAA) requires physicians and other providers to comply with a detailed set of privacy and security regulations regarding patient health information. When HIPAA went into effect in 1996, it was designed to help employees who change jobs to keep their health insurance by making their coverage portable. Congress then broadened the law to include the privacy and security of patient information.

The HIPAA security standards require physicians to keep medical information about patients private, to protect the data against any reasonably anticipated threats or hazards, to prevent any mishandling of the information and to ensure compliance by training all staff members.

The HIPAA security rule involves three types of safeguards. The administrative safeguards include assessing the security of your computer system, training staff on security procedures and developing business associate contracts that address the security of electronic medical data. Compliance with these standards involves a number of steps, such as the following:

- Perform and evaluate background checks on employees.
- Lock file cabinets that contain patient health information, or keep them in a locked room.
- Utilize encryption of electronic data sent over the Internet.
- Secure fax machines so messages can't be read by passers-by.
- Use passwords on all computers that maintain personal information, and ensure that computer passwords are not shared or kept near the computer.
- Establish a system of sanctions for individuals who violate the practice's privacy policies.

If your computer is attached to a network, it is important to make sure that the network is protected by a firewall, writes Dr.

### **HHS Debunks Some HIPAA Myths**

In May 2004, the Department of Health and Human Service's Office for Civil Rights issued guidance to healthcare providers clarifying the following misconceptions about the HIPAA privacy rule:

- HIPAA does not require patients to sign consent forms before doctors, hospitals or ambulances can share information for treatment purposes. Providers can freely share information with other providers where treatment is concerned, without getting a signed patient authorization or jumping through other hoops.
- HIPAA does not require providers to eliminate all incidental disclosures. The privacy rule was modified in August 2002 to clarify that incidental disclosures—such as those that may occur through the use of office sign-in sheets—do not violate the rule when physicians have common-sense policies that reasonably safeguard and appropriately limit how protected health information is used and disclosed.
- HIPAA does not cut off all communications between providers and the families and friends of patients. Doctors can share needed information with family and friends, as long as the patient does not object. The privacy rule also makes it clear that, unless a patient objects, doc-

David C. Kibbe, director of the American Academy of Family Physicians Center for Health Information Technology, in an April 2005 article in *Family Practice Management*. In addition, you should obtain assurances from business associates that they will secure the electronic health information they create, maintain or transmit on your behalf. These relationships include insurance companies, transcription and billing services, hospitals, laboratories and Internet service providers.

When faxing records to another office, have office staff telephone first to be sure that the fax number is correct and that the intended receiver will be present to accept the information as it arrives. Further, patients can be asked to put their names and the time of arrival on a sign-in sheet in the office as long as they don't disclose the reason for their visit on the sheet. If you must discard paper records, experts recommend you purchase an inexpensive shredder to shred these documents to assure patient privacy.

Make certain that everyone in the medical office takes the HIPAA security regulations seriously. "Most security breaches

tors, hospitals and other providers can disclose information when needed to notify a family member, or anyone responsible for the patient's care, about the patient's location or general condition. Even when the patient is incapacitated, a provider can share appropriate information for these purposes if he or she believes that doing so is in the best interest of the patient.

- HIPAA does not stop calls or visits to hospitals by family, friends, clergy or anyone else. Unless the patient objects, basic information about the patient can still appear in the hospital directory, so that when people call or visit and ask for the patient, they can be given the patient's phone and room number and general health condition.

- HIPAA does not prevent child-abuse reporting. Physicians may continue to report child abuse or neglect to the appropriate government authorities.

- HIPAA is not anti-electronic. Doctors can continue to use e-mail, telephones or fax machines to communicate with patients, providers and others using common-sense, appropriate safeguards to protect patient privacy.

Log on to [www.hhs.gov/ocr/Healthcare-Provider-letter.pdf](http://www.hhs.gov/ocr/Healthcare-Provider-letter.pdf) for additional information.

occur when insiders—people working for the organization—exercise faulty judgment or fail to follow protocols in which they've been trained," Dr. Kibbe writes.

The HIPAA privacy rule regulates how medical practices use and disclose patient information, whether it is spoken, written or electronic. This information involves paper records and oral communications as well as e-mails, faxes and electronically stored or transmitted information.

**The individual you designate as the privacy official must monitor the various steps your office takes to comply with HIPAA. The privacy official must also make sure that current and new staff members are trained on how to comply with HIPAA regulations as they apply to your practice.**

The privacy rule gives patients more control over their health information and sets boundaries on the use and release of health records. It generally gives patients the right to examine and obtain a copy of their own health records and to request corrections.

There are a number of regulations that you must follow to be in compliance with HIPAA's privacy standards:

- Designate someone on your staff to be in charge of compliance.
- Obtain a patient's written consent for use and disclosure of patient information for treatment, payment and healthcare operations at the patient's first encounter with you.
- Make sure that only the minimum necessary health information be used or disclosed.
- Establish policies regarding the types of uses and disclosures of medical data that the practice is allowed to make for purposes of treatment, payment and healthcare operations.
- Train and educate your staff about these policies and compliance with the privacy rule.

In addition, make it clear to patients in writing that protected health information can be released to public health authorities that are authorized by law to collect information for a number of purposes including reporting child abuse or neglect; preventing or controlling disease, injury or disability, and maintaining vital records such as births and deaths.

Your medical office has probably already developed a notice of privacy practices for patients, which they receive at the first

office visit. The law requires that your practice obtain patients' written acknowledgement that the privacy notice has been received and read.

The individual you designate as the privacy official must monitor the various steps your office takes to comply with HIPAA. The individual must also make sure that current and new staff members are trained on how to comply with HIPAA regulations as they apply to your practice.

### **Satisfying the HIPAA Training Requirement**

When conducting HIPAA training, it is a good idea to teach your staff how to follow your organization's policies and procedures; how these policies and procedures deal with privacy and security issues, and what to do if they have questions or concerns, says Neil B. Caesar, president of the Health Law Center, a national health law firm headquartered in Greenville, S.C.

Memos and written information can be used to provide occasional alerts to staff, but they do not replace good training programs that are professionally conducted by you or the other leaders in your practice, he explains.

Nevertheless, the government says the HIPAA training requirement may be satisfied in a small practice by providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies. A large health plan may provide training through live instruction, video presentations or interactive software programs.

Keep in mind that HIPAA does not require the same training for all personnel in your office, Mr. Caesar says. For example, the receptionist, the patient appointment scheduler or the floor nurse needs only be familiar with a few policies that affect him or her on a daily basis.

If you decide to do your own in-house training, Mr. Caesar recommends that you establish clear objectives and explain the practical relevance of these objectives. You may choose to conduct the training off-site, providing lunch or refreshments, he says.

It is important that your staff know that a HIPAA complaint by a patient or other affected person can result in serious consequences for both your practice and the employee. If they understand the seriousness of the law, they are more likely to become active participants in any training sessions you provide.

The federal government says that the privacy official at a small physician practice may be the office manager, who will have other non-privacy related duties. The privacy official at a large health plan may be a full-time position and may have regular support and advice of a privacy staff or board.

With regard to electronic transactions, make sure your software and those of the entities you deal with are HIPAA compliant. Many

**If a patient experiences a problem related to the privacy of his or her medical information, he or she can file a formal complaint with HHS. The Department has the authority to impose civil and criminal penalties if it finds a violation of the law. Patients must file complaints within 180 days of the incident.**

software vendors have devised software to meet the HIPAA regulations. If you need details regarding specific practice management software vendors, visit [www.hipaa.org/pmsdirectory](http://www.hipaa.org/pmsdirectory) for information supplied by the vendors themselves. Some companies provide integrated packages of software, hardware and training and assessment services to help physicians and healthcare organizations comply with HIPAA requirements.

Keep in mind that if a patient experiences a problem related to the privacy of his or her medical information, he or she can file a formal complaint with HHS. The Department has the authority to impose civil and criminal penalties if it finds a violation of the law. Patients must file complaints within 180 days of the incident.

So far, HHS's compliance and enforcement activities are prompted by complaints, though the agency says that it may also conduct reviews to determine if a covered entity is in compliance. When a complaint is made, HHS says that it attempts to resolve the matter informally by providing technical assistance to the healthcare provider or establishing a corrective action plan.

"Resolving issues through such informal means is often the quickest and most effective means of ensuring that the benefits of the HIPAA rules are realized," HHS says. "However, if we are unable to obtain compliance effectively on matters within our jurisdiction through voluntary means, we may seek to impose civil money penalties. Moreover, matters subject to criminal penalties are referred to the Department of Justice."

According to a 2005 survey conducted by the Healthcare Infor-

mation and Management Systems Society and Phoenix Health Systems, 78 percent of providers—hospitals and medical practices—stated that they were in compliance with HIPAA's privacy rules; 18 percent of providers reported that they remain non-compliant more than two years after the deadline. Twenty-one percent of providers said that they had had formal complaints of privacy violations filed against them, either with the federal government or in a civil proceeding, over the past six months.

Violation for noncompliance with HIPAA standards is \$100 per violation to a maximum of \$25,000 per year for each type of violation. For privacy standards, criminal penalties range from fines of \$50,000 and/or one year in jail to \$250,000 and/or 10 years in jail for knowingly using individually identifiable patient data with malicious intent or for financial gain. Further, patients may sue under tort law for invasion of privacy, breach of duty or confidentiality or negligence claims existing under state law.

It is important to realize that malpractice and standard liability insurance policies do not cover federal penalties or tort liability claims arising from injury attributed to lost, stolen or misused medical information. A plaintiff can file a lawsuit against you by alleging a breach of the federal statute. Other possible suits may result from alleged negligent disclosure of protected health information, negligent supervision and training of employees and loss of occupation or wages caused by release of protected information.