

Fraud and Abuse Implications for the HIM Professional

Save to myBoK

by Sue Prophet, RRA, CCS, director of classification and coding

Healthcare Fraud and Abuse Legislation

On August 21, 1996, President Clinton signed into law the Health Insurance Portability and Accountability Act. This law addresses several issues including the creation of a Health Care Fraud and Abuse Control Program. This program is intended to combat fraud and abuse in the Medicare and Medicaid programs, as well as in the private healthcare industry. It will be coordinated by the Office of the Inspector General and the Department of Justice. The Office of Inspector General (OIG) and the Department of Justice have been given the power to enforce federal, state, and local laws to control healthcare fraud and abuse and to conduct investigations and audits pertaining to the delivery of and payment for healthcare services.

The Office of Inspector General, which is part of the Department of Health and Human Services, was established by Congress in 1976 to identify and eliminate fraud, waste, and abuse in Department of Health and Human Services programs and to promote efficiency and economy in departmental operations. This mission is carried out through a nationwide program of audits, investigations, and inspections.

The Department of Justice includes the Federal Bureau of Investigation and US Attorney offices. Other official entities that may be involved in conducting fraud and abuse investigations include the Attorney General, state Medicaid fraud control units, Medicare fiscal intermediaries, and private insurance carriers.

According to the Health Insurance Portability and Accountability Act, criminal penalties will be imposed on healthcare professionals who "knowingly and willfully" attempt to execute a scheme to defraud any healthcare benefit program or to obtain, by means of false or fraudulent pretense, money or property owned by, or under the custody of, a healthcare benefit program. Criminal penalties of up to 10 years imprisonment may be imposed. If the violation results in serious injury to a patient, the healthcare professional will face up to 20 years imprisonment and possible life imprisonment if the death of a patient results from the violation.

The civil monetary penalty for healthcare fraud has been increased from \$2000 to \$10,000 for each item or service for which fraudulent payment has been received. The monetary assessment has been increased from not more than twice the amount to not more than three times the amount of the overpayment. Two practices have been added to the list of fraudulent activities for which civil monetary penalties may be assessed:

1. Engaging in a pattern of presenting a claim for an item or service based on a code that the person knows or should know will result in greater payments than appropriate
2. Submitting a claim or claims that the person knows or should know is for a medical item or service that is not medically necessary

There are approximately 2000 cases in the Health Care Financing Administration's (HCFA) Medicare fraud investigation database.

Qui Tam Litigation

You may have heard the term "qui tam lawsuit" in reference to a fraud and abuse investigation. Qui tam litigation (also known as the "whistle-blower" statute) allows private citizens to act on the government's behalf in filing lawsuits claiming that a party has violated the Federal False Claims Act by filing false claims with the federal government or under federally funded programs. The False Claims Act prohibits knowingly presenting false or fraudulent claims to the government. In this context, "knowing" means actual knowledge of the falseness or fraudulence of the claim, or deliberate ignorance of the truth, or

reckless disregard for the truth. Qui tam plaintiffs may be anyone who has knowledge about the coding, billing, or general financial operations of a provider. Potential whistle-blowers include current or former employees, beneficiaries, independent contractors, and consultants. Whistle-blowers are protected from employer retaliation through federal or state "whistle-blower" laws. To encourage whistle-blowers to come forward, the government may award them between 15 percent and 25 percent of the funds it recoups.

What Does This Legislation Really Mean?

Some of the language in the Health Insurance Portability and Accountability Act has resulted in some confusion and misinterpretation. One fraudulent practice is defined as engaging "in a pattern of presenting a claim for an item or service based on a code that the person knows or should know will result in greater payments than appropriate." Does this mean when you and the Peer Review Organization disagree on the principal diagnosis for a case that you could be guilty of fraud? No! There must be a *pattern*. Errors and random differences of opinion are permitted. It is only when there is a pattern of an inappropriate code or DRG assignment that you need to be concerned about fraud charges.

What does "know or should know" mean? If instructions concerning the coding or billing practices in question have been published and disseminated by the federal government or your fiscal intermediary (such as in a provider bulletin), you "should know." If the issue is addressed in official ICD-9-CM coding guidelines (as published in *Coding Clinic*) or in the CPT rules (contained in the CPT book), you "should know." Lack of personal knowledge because the provider bulletins came to the business office and were never disseminated to the HIM department or because your facility chose not to subscribe to *Coding Clinic* is not a justifiable defense. As far as the authorities are concerned, the pertinent payment policies and official coding guidelines were published and available and you "should know."

Here is an example of the intent of this legislation and how it works:

A hypothetical fraud investigation targets the principal diagnosis code assignment for patients admitted with urinary tract infections. Coding guidelines state the urinary tract infection code must be sequenced before the code for the organism. However, if the organism code is sequenced first, the patient is assigned to a higher-weighted DRG. Data from Hospital A reveals that in a couple of cases the organism code was sequenced first, but in the vast majority of cases the code for urinary tract infection was sequenced first. At Hospital B, the organism code was sequenced first most of the time. Hospital A would not be charged with fraud because no pattern is established. The few instances of sequencing the organism code first were most likely errors. However, there is clearly a pattern at Hospital B, so fraud charges would be filed. Hospital B might try to defend itself by saying a consultant advised it that sequencing the codes in this manner was acceptable or maybe all the coders went to a seminar and learned this practice was permissible. However, the appropriate sequencing is addressed in *Coding Clinic*, which is the only official source of ICD-9-CM coding advice. Hospital B might claim it was unaware of this official guideline, but the "should know" criterion applies.

Another type of fraudulent activity defined in the new legislation is "submission of a claim for a medical item or service that you know or should know is not medically necessary." How is medical necessity determined? Medical necessity can be substantiated by the presence of an appropriate diagnosis code on the claim, a physician's order containing the reason for the test, or other physician documentation of the need for the service. "Rule-out" and "suspected" diagnoses do not provide documentation of medical necessity. Ironically, the current fraud and abuse initiatives are pushing for improved documentation in areas where HIM professionals have been demanding it, often with little or no success, for a long time. How many times have you told physicians or the administration, admitting, laboratory, and radiology departments that you needed physician orders and the reason for the test when patients presented for ancillary tests? How often have you explained to physicians that you cannot code "r/o pneumonia" for a visit for a chest x-ray?

It is important to note that penalties for fraud are assessed against the provider, not individual employees. The provider is the entity that has benefited from collection of the fraudulent payments. Consulting firms whose fees are based on the additional reimbursement "found" during medical record audits can also be drawn into fraud investigations and may be assessed penalties as well.

Risk Areas for Coding Fraud

- DRG assignment
- Unbundling (assigning separate codes for each component of a comprehensive service to increase reimbursement)

- Assigning a code for a higher level of service than the service actually provided
- Assigning a code for a "covered" service when the service actually provided is "non-covered"
- Assigning codes for diagnoses that are not present or for procedures that were not performed
- Discrepancies between the physician's and hospital's codes for the same patient visit

When appropriate, the OIG issues "Special Fraud Alerts" to identify segments of the healthcare industry that are particularly vulnerable to abuse. These alerts notify the industry that the OIG has become aware of certain abuses and plans to pursue and prosecute such cases or bring civil and administrative action against such facilities. They offer an opportunity for providers to examine their own practices in these areas.

Fraud investigators review lots of data from huge databases, such as HCFA's MEDPAR file, looking for providers who are "outliers." Outlier providers are those whose coding or billing practices are significantly outside the norm. For example, if the percentage of cases assigned to a particular DRG is usually 10 to 15 percent, but in your facility, 60 percent of cases are assigned to that DRG, your facility could become a target of a fraud investigation. If the percentage of patients assigned the highest-level Evaluation and Management (E&M) codes is considerably higher than for other physicians in the same specialty, that physician could become a target of an investigation. Statistical data over several years may be reviewed by investigators. Any significant changes in case mix or coding or billing practices can be cause for suspicion.

If a whistle-blower identifies a possible fraudulent practice in one healthcare organization, investigators may examine national or state data from many facilities to identify other providers who might be involved in the same practice. If a facility involved in an investigation is owned by a corporation, the investigation may be broadened to encompass all facilities owned by this corporation because the questionable practice may reflect corporate policy. If a provider's fraudulent activity is the result of a consultant's recommendation, the investigation may encompass all of that consultant's clients.

As you can see, a provider can easily become the target of a fraud investigation without anyone pointing a finger directly at him or her. If you find yourself embroiled in an investigation, don't panic. An investigation is just that, an investigation. It does not necessarily mean you have done anything wrong. However, it does not help matters if you have little or no knowledge of your current coding or billing practices; there are few policies/procedures (or they are outdated); and you are unable answer the investigators' questions or provide them with the information necessary to prove fraud charges are unfounded. By incorporating the following steps in your daily operations, you can minimize your risk of being the target of an investigation and maximize your chances of emerging triumphant if you are involved in an investigation.

Fraud and Abuse Prevention Strategies

- Make sure that all coding staff have been properly trained and receive ongoing continuing education.
- Develop comprehensive internal policies and procedures for coding and billing and make sure these written procedures are kept up-to-date. Provide training with regular refresher courses to staff. Conduct random, periodic reviews to make sure procedures are being followed. Keep records of these reviews and their conclusions. Establish mechanisms for all staff to be updated on changes *before* the effective date of the change. Keep records of all staff in-services, including signatures of staff members acknowledging their participation in the training session and their understanding of the policies and procedures. If you disseminate a memo describing a revised policy or procedure change, ask staff to sign the memo acknowledging their receipt of the information. Keep the memo and the staff signatures on file.
- Monitor coding accuracy through quality audits. Use these audits to identify gaps in knowledge or weak areas and provide appropriate training.
- Evaluate your internal coding practices, and assure they are consistent with coding rules and guidelines. Many facilities have developed facility-specific coding guidelines, which is fine as long as they don't conflict with the official guidelines. Official coding guidelines take precedence over any other guidelines.
- Compare diagnosis codes with procedure codes for consistency.
- Compare reported diagnosis and procedure codes with documentation in the medical record.

- For Evaluation and Management code assignment, compare the required components of the reported E&M code with the documentation in the medical record to assure the code level assigned is substantiated.
- When documentation deficiencies are identified, educate the physicians on improving their documentation. Emphasize the initial importance of documentation by showing examples of how poor documentation can lead to adverse consequences.
- When clarification or additional information is obtained from the physician for coding purposes, make sure this information is subsequently documented in the medical record. Most coders are familiar with the coding principle of "query the physician" when documentation affecting code assignment is unclear or incomplete. Too often, the physician answers the coder's query verbally (or via a note) and the code is assigned based on this exchange, but the physician never adds the information to the record. Thus, the medical record documentation does not support the code assignment. It is not going to help a fraud investigation to tell an investigator "I asked the physician if it was okay to add a code for that condition, and he approved it." The condition *must* be documented in the medical record.
- Establish a mechanism to assure that memorandums on regulatory issues and provider bulletins are disseminated to all affected staff. The business office is not the only department that needs to know this information. The staff performing the coding and billing functions, not just managerial staff, need to receive this information.
- Do not automatically implement a coding or billing practice simply because a consultant or seminar instructor recommends it. The title of "consultant" or "instructor" does not necessarily make this person more of an "expert" than you. And while there are plenty of reputable firms, there are also some not-so-reputable ones. Verify that the recommendation does not conflict with current official coding guidelines or payment policy. Keep in mind that any abrupt shift in coding or billing practices could make you a target for a fraud investigation, so it is especially important that your change in practice can be supported.
- Keep up-to-date on government regulations (no easy task!). As new or revised regulations are published, add this information to your coding or billing policy and procedure manual. Maintain an up-to-date index for this manual so information is easily accessible for staff.
- Become familiar with physician and/or hospital billing, (depending on which type you are involved in) patterns of utilization, and norms for claims data. Compare your physician's E&M code usage pattern with other physicians in his specialty in the region, state, or nation. Compare your facility's DRG distribution with national data. Compare closely related DRGs. Do you have a significantly higher percentage of patients assigned to a particular DRG than the national or state average? If so, be particularly concerned if this DRG has a higher weight than most of the other DRGs in its "family." Look into the reasons why so many patients are assigned to this DRG. There may be a perfectly logical explanation, and all the cases assigned to this DRG may be appropriate. However, this statistical aberration may attract the attention of the authorities. If you become the target of an investigation, you will be at an advantage if you have already conducted an investigation and feel confident that nothing will be found wrong with your coding practices.
- Evaluate claims denials and code and DRG changes from the fiscal intermediary and Peer Review Organization. Use this information, such as patterns of errors, as an opportunity to educate staff. Appeal all denials you believe to be inappropriate, even those involving only small amounts of money.
- Examine your organization's data over the past several years. Have there been any significant changes in case mix or coding practices? Any significant increases in the number of patients assigned to some DRGs (particularly DRGs that are higher-weighted than their related DRGs)? Are there reasonable explanations for this shift? Document any explanations. Keep in mind that any sudden changes in patterns can raise a red flag in the minds of the authorities, and fraud investigations can go back several years.
- Make sure your chargemaster is being maintained by someone with knowledge of coding, billing regulations, and medical record documentation.

- If you identify an inappropriate coding or billing practice that could be construed as fraud (i.e., it resulted in overpayments), inform your legal counsel of any adverse implications and let them decide the appropriate course of action. A compliance program to correct the problem and assure it doesn't recur should be implemented at once-before your facility becomes a target of an official fraud investigation.

What Should You Do If Are Asked to Implement a Coding Practice You Believe to Be Fraudulent?

1. Compile documentation (for example, issues of *Coding Clinic*) supporting your position.
2. Meet with your supervisor to discuss the issue. Show him or her the documentation supporting the inappropriateness of the coding practice in question. Discuss the potential implications of implementing this practice (e.g., fraud charges).
3. If the meeting with the supervisor is unsuccessful, arrange a meeting with the department director. If this meeting is also unsuccessful in resolving the issue, meet with the administrator to whom your department director reports.
4. If your facility is owned by a corporation, you might consider taking the issue to the corporate level if you are unable to resolve it internally.
5. You might consider suggesting that an objective third party (such as a consultant you trust and respect) be brought in and asked for their opinion.
6. If all of these efforts are unsuccessful, and you are still being asked to implement the coding practice, send a memo to your supervisor, department director, CFO, and CEO. Keep a copy for your files. In this memo, describe the issue, your opposition to the coding practice and reasons for your opposition, and all of your efforts to date to resolve the matter. Cite all official sources backing your position. Since the CFO and CEO may not be familiar with coding guidelines, explain what "official coding guidelines" are and who approves them (i.e., the four Cooperating Parties-National Center for Health Statistics, Health Care Financing Administration, American Hospital Association, and American Health Information Management Association). Explain the potential for fraud charges and the penalties involved. You might also mention the AHIMA Code of Ethics and your professional obligation to abide by it. While there is no guarantee this memo will prevent the coding practice from being implemented (or continuing), it will help to protect you from becoming the scapegoat if the facility is ultimately charged with fraud. It will also help to prevent your professional conduct from being questioned.
7. Depending on the seriousness of the issue, you may wish to consider terminating your employment at this facility in order to avoid being associated with the fraudulent practice in any way. If fraud charges are brought against this facility and if there is publicity surrounding the case, you could find yourself in an untenable position. Your opposition to the fraudulent practice may not be as widely known as the fact you are a coder from the facility charged with coding fraud. This reputation could make job hunting very difficult.
8. If you decide to become a whistle-blower, consider all of the ramifications very carefully. Although laws protect whistle-blowers from employer retaliation, it could be very difficult for you to continue working at that facility. Whistle-blowers are often considered a threat in the business community, so you could find yourself blackballed and unable to find another job. Since whistle-blowing can have serious consequences, both for you personally as well as the healthcare organization, make sure you have sufficient documented evidence of the fraudulent activity before blowing the whistle.

Every situation is different and requires you to think through your various options and consider very carefully how you wish to proceed. However, keep in mind that the AHIMA Code of Ethics states "the HIM professional refuses to participate in illegal or unethical acts and also refuses to conceal the illegal, incompetent or unethical acts of others." Therefore, you have a professional responsibility to refuse to participate in or refuse to ignore fraudulent activities.

OIG Online

The Office of Inspector General's Work Plan for Fiscal Year 1997 is now available on the Internet. Among the projects listed in this work plan is examination of DRG miscoding. OIG will undertake a review to determine the extent to which hospitals are

incorrectly coding hospital discharges for Medicare payment. An approach will be developed to target facilities possibly engaged in inappropriate coding for more thorough review and remedial action. OIG may use changes in case mix or commercial software to detect billing irregularities. The entire 110-page work plan can be downloaded from the Small Business Administration's Web site at <http://www.sbaonline.sba.gov/ignet/internal/hhs/hhs.html>.

Article citation:

Prophet, Sue. "Fraud and Abuse Implications for the HIM Professional." *Journal of AHIMA* 68, no.4 (1997): 52-56.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.