Compliance, Medical Records, and the FBI: Preventing Fraud and Abuse

by L. Stephan Vincze, JD

The possibility of an investigation related to fraud and abuse is the last thing most people want to think about, but it's important to be prepared, just in case. The author gives some advice on how to react if your facility is the target of an investigation and points out some important steps to take to ensure compliance.

Imagine the following: You're a professional in charge of your local hospital's health information management (HIM) department. One morning, you learn that the FBI would like to speak to you about your hospital's medical records. A special agent presents you with a search warrant issued by a magistrate in the US District Court, asking to review records, computer files, and disks covering a six-year time frame.

They would like your full cooperation. How should you react?

Hopefully, this scenario will never happen to you. If it does, however, you need to be prepared. Taking appropriate compliance measures and ensuring that your HIM department is an integral part of your organization's compliance program are important steps toward preparation.

Healthcare Fraud and Abuse: Some Background

An Increasingly Hot Topic

The best way to avoid the above scenario is through preventive measures. This shouldn't be a surprise—fraud and abuse has become an increasingly hot topic and fraud prevention is now an organizational imperative. Today, the definition of fraud reaches beyond the classic understanding that requires a willful and knowing intent. Rather, today you may have a "reckless disregard" of the circumstances or exhibit "willful ignorance" to be subject to prosecution under the Federal False Claims Act. With "compliance" a buzzword in healthcare today and issues related to fraud well publicized, not having a systematic process to detect and prevent fraud and abuse (i.e., a compliance program) could arguably equate to "reckless disregard" of current circumstances. Explaining that you and your staff just didn't know that DRG-79 upcoding is a problem that warrants attention may be construed as "willful ignorance."

With new regulation and public laws coming to the fore, HIM professionals and their organizations are subject to scrutiny as never before. Most of this attention is rooted in initiatives to save money and eliminate waste. In 1996 alone, the Medicare program is estimated to have lost $23 billion, or 12 percent of total Medicare payments for that year, because of fraud. Moreover, the government has estimated total healthcare fraud to equal approximately $100 billion per year—or 10 percent of all healthcare revenues.[1]

Laws such as the Health Insurance Portability and Accountability Act (HIPAA) have brought the issue further into the spotlight, expanding the enforcement powers of federal regulators, prosecutors, and law enforcement authorities. Even the Balanced Budget Act of 1997 has a total of 15 sections that address fraud and abuse.

Whether or not the FBI pays your organization a visit, you need to know some of the basic considerations of "effective compliance." It's important not only to be in compliance, but also to be able to demonstrate that you, as an HIM professional, are taking the appropriate "due diligent steps" to stay in compliance.

Enforcement--The FBI and Search Warrants

If an investigation does take place, you are likely to be confronted with a search warrant. The Fourth Amendment of the US Constitution requires that warrants authorizing a search be based on probable cause that is supported by sworn testimony or a sworn affidavit that describes with specificity the place and evidence to be searched and seized. It is not difficult to get a search warrant—they are issued by magistrates to law enforcement officials who then execute the warrant. It is imperative that you establish clear protocols and policies on how to respond to a government investigation, just in case.

How to Respond to a Search Warrant

I recommend that as a general matter you proceed with the following steps:

1. Politely respond to the special agent that you will certainly cooperate, but that before you can answer any more questions or provide any other assistance, you must first speak to your attorney.
2. Ask for some privacy and call your organization's general counsel or other designated lawyer. Inform the attorney what has happened and request that he or she or another attorney come to your office to assist you as soon as possible.
3. Inform the FBI agent that your counsel is on the way. With a properly authorized search warrant, the agent does not have to wait for counsel to arrive to start collecting the evidence specified in the warrant. Cooperate with the agent's request to collect the specified records and information. Do not, however, answer any more questions until counsel arrives. If pressed, politely decline and inform the agent that you want to ensure that you proceed properly and appropriately and wish to have the advice of counsel prior to responding to any further questions. Legally, the agent should honor your request.

The Significance of a Search Warrant

Are you and your organization necessarily in jeopardy by the mere fact that a search warrant has been issued? Generally, the issuance of a search warrant is a sign that the FBI has uncovered significant incriminating evidence. However, courts have thrown out evidence if a search warrant was based on unreliable or fabricated evidence. A recent case involving a home health agency was dismissed due to false statements used to authorize a search.[2] You should not count on that happening, however. FBI agents in particular are well schooled in the law of search and seizure, and errors in that process are the exception, not the rule. Generally, before you become aware of an investigation, it will have already been under way for six to 12 months.

Typically these types of fraud investigations start with a phone call from an employee who believes that something improper is being done and that the organization has no intention, desire, or mechanism to address it. Accordingly, the employee feels compelled to report the perceived improper conduct to law enforcement authorities. After making initial contact, the potential "whistleblower" is typically called in for a series of interviews to determine his or her veracity and credibility. If the employee's concerns seem to be reasonable, plans will be made to obtain corroborating evidence.

The Role of Compliance Programs

The real challenge for HIM professionals is ensuring that your department is prepared to address fraud and abuse before any law enforcement agency becomes involved. I recommend that you take the following steps to start:

1. Conduct a risk assessment of your medical records department. A quality assessment can provide a strategic road map to the gaps and weaknesses you need to address and the strengths you can build on. If you ask someone from outside to review past records, you should secure the engagement through your legal counsel to ensure that reports of audit findings are protected under the attorney-client privilege.
2. Insert yourself into the compliance efforts of your organization. When it comes to implementing compliance programs, hospitals often focus only on the overarching process, the program's framework, and associated legal documents. HIM professionals have numerous skills and capabilities that should make them key players in compliance efforts. Seek out a meeting with the compliance officer, if there is one, and the general counsel. Express your concerns and recommend that your department participate in focus group meetings that help design the standards of conduct and subsequent training. Also, recommend that specific technical training related to proper coding and documentation requirements be part of the compliance program and that it be specifically designed to meet the needs of your employees. Use this article and others like it to support your case.

3. Review your document retention/destruction and confidentiality policies with counsel. There may be documents that should be appropriately protected from searches and seizures. It is important to identify such documents with the aid of counsel and to clearly mark them and store them in a secure manner. Confidentiality of medical records is also a high-risk area if effective policies are not in place. Reviewing your confidentiality policies and procedures should be near the top of your list.
4. Educate yourself on HIM compliance requirements. Attendance at a current training program focused on HIM compliance requirements is evidence of your sincere effort to remain current with the ever-changing regulatory environment. Mere attendance, however, is not enough. Follow through by sharing what you have learned with your staff at a scheduled meeting or training session.
5. Start now and document the steps you take. The sooner you start, the better off you will be. The credibility of your efforts to do everything possible will be enhanced. Keep a chronology of all the compliance-related measures taken for your department. Within a relatively short period of time, you will have a catalogue of proactive measures that you have implemented. Again, this is evidence of a sincere commitment to take the necessary "due diligent steps" to establish an effective compliance program.

Conclusion

The key to overcoming fear is proactive preparation based on knowing what threats exist and how your organization is prepared to meet them. If you start with the suggested steps outlined in this article, you should have the confidence of knowing that you have taken the necessary "due diligent steps" to be in compliance and to prevent and detect fraud and abuse.

Notes

1. Cole, David. "Managed Care Facts and Figures." *Medical Interface* (June 1996): 62-63.

2. Healthcare Financial Management Association and Atlantic Information Services. *Report on Medicare Compliance* vol. 6, no. 32. Washington, DC: 1997.

L. Stephan Vincze *is an attorney and vice president of compliance services with Healthcare Management Advisors, Inc. (HMA), in Atlanta, GA.*

Article Citation:
Vincze, Stephan L. "Compliance, Medical Records, and the FBI: Preventing Fraud and Abuse." *Journal of AHIMA* 69, no. 1 (1998): 40-42.