Compliance Programs: Beyond Billing and Coding

Save to myBoK

by Odell Guyton, JD

Ensuring the success of your compliance program means keeping your eye on more than billing and coding. The author highlights some issues on the horizon for compliance officers.

As a compliance officer of your healthcare organization, you've established your formal compliance program and it's up and running. But is your work finished? The answer is no. Beyond the perennial challenges presented by billing and coding issues, healthcare organizations need to be aware of other factors that affect compliance programs. In this article, we'll discuss the implications of HIPAA for compliance programs, consider the impact of research, and learn how to assess your risk.[1]

The Impact of HIPAA

The government's war on healthcare fraud and abuse will continue to challenge compliance programs by emphasizing accountability at the highest levels of the organization.

While the Department of Justice (DOJ) and Office of the Inspector General (OIG) have always been active in investigating allegations of healthcare fraud, many other federal and state agencies have now joined in a parallel effort. Law enforcement's emphasis will most likely be directed to continuing use of existing fraud statutes and the federal False Claims Act. The Department of Health and Human Services (HHS) and the OIG continue to press for individual physician practice compliance, quality healthcare initiatives, and the implementation of the administrative simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA), especially the privacy provisions.[2]

Other aspects of the HIPAA law should not be underestimated. HIPAA creates additional risks, because it permits the government to exclude managers and officers of a physician practice or other healthcare entity based on organizational misconduct. An exclusion under these circumstances will prohibit these individuals from having any position or relationship with a healthcare entity that provides items or services to federally funded programs, including Medicare, Medicaid, and CHAMPUS. Furthermore, HIPAA has expanded the definition of "healthcare fraud" to include fraud to private healthcare payers as well as public.

Other government agencies have echoed the demand for improved systems for internal controls. Agencies such as the National Institutes of Health (NIH) are moving from a model of reactive to proactive compliance and have moved to make zero-tolerance compliance an "institutional expectation" through increased focus on management controls and performance assessments.

Keep an Eye on Research Programs

Research deserves the heightened attention of compliance professionals at both the financial accountability and regulatory levels. Activities of scientific misconduct, if serious, may ultimately lead to a person's or organization's "debarment" or exclusion from receiving federal funding, including grants and other subsidies, for up to three years. This issue is receiving more attention nationally, because since 1999 HHS has announced several changes designed to improve its processes for responding to allegations of research misconduct and promoting research integrity.

As a proactive step, organizations where research programs take place may wish to build these programs into their compliance agenda. The first step is a strategic research compliance risk assessment. The common research risks include the following:

- protection of human subjects volunteers with a focus on institutional review board compliance
- investigator conflict of interest

- Medicare billing compliance
- cost sharing and cost transfers
- time and effort reporting

Enhanced protection against retaliation to whistleblowers, impact to reputational risks through negative press, and False Claims Act exposure should be top considerations on the risk assessment.

Understanding IRBs

Institutional review boards (IRBs) are under particular scrutiny these days. Last year, former HHS secretary Donna Shalala referred to IRBs as the key element of the system to protect research subjects. The government views IRBs as under increasing strain and victims of excessive workloads and inadequate resources.[3]

OIG reports issued in 1998 and 2000 have questioned the effectiveness of IRBs in protecting human research subjects.[4] Both reports are critical of how the FDA and Office for Protection from Research Risks (now the Office of Human Research Protections) have taken no action on an OIG recommendation to require IRBs to have adequate resources to carry out their duties. As a proactive measure, compliance professionals may wish to build research into their compliance program by evaluating whether their institution has devoted adequate financial and human resources to the IRB function so that the IRB may effectively perform its duties.

Inadequate funding of an IRB's resources may place your institution at risk. A resource evaluation is recommended. In conducting a resource evaluation, it is helpful to understand an IRB's role when approving research.

IRBs determine whether:

- risks to subjects are minimized:
    - by using procedures that are consistent with sound research design and that do not unnecessarily expose subjects to undue risk
    - whenever appropriate, by using procedures already being performed on the subjects for diagnostic or treatment purposes
- risks are reasonable in relation to anticipated benefits to subjects, if any, and to the importance of the expected knowledge. In evaluating risks and benefits, the IRB considers only those risks and benefits that may result directly from the research
- selection of subjects is equitable. In making this assessment, the IRB considers the purpose of the research and the setting in which the research will be conducted
- informed consent will be sought from each prospective subject or the subject's legally authorized representative unless waived in accordance with regulations
- informed consent will be appropriately obtained and documented, usually with a signed written consent form
- the research protocol makes provisions for monitoring the data collected to ensure the safety of subjects
- there are provisions to protect the privacy of participants and to maintain the confidentiality of data

There are additional safeguards to protect the rights and welfare of subjects when some or all of them are likely to be vulnerable to coercion or undue influence (children, prisoners, pregnant women, handicapped, mentally disabled persons, or economically and educationally disadvantaged persons).

The government has identified six general areas that jeopardize the effectiveness of IRBs across the country. It is believed that some of these factors may have contributed to enforcement actions resulting in shutdowns at research institutions. Keep these factors in mind as you evaluate the strengths and weaknesses of your institution.

The concerns are as follows:

- changes in the research environment. Research financial conflicts of interest, increased number of research proposals, proliferation of multisite trials, and new types of research have created significant changes in the research environment
- IRBs review too much, too quickly, with too little expertise. Increased work load, lack of resources, insufficient deliberation over protocols, and failure to gain access to scientific expertise contribute to this factor

- minimal continuing review of approved research is conducted with too little information about how the actually research is being conducted post approval.
- conflicts threaten IRB independence. Institutions rely on the prestige and revenue generated by the research. They expect IRBs to support the interest of the institution and protect human subjects at the same time
- investigators and IRB members receive little training
- little attention is devoted to IRB effectiveness

The role of the compliance professional will become more complex as compliance programs and officers become more recognized by management as an institutional resource to protect the corporate entity from liability, and compliance officers assume a greater role of institutional risk manager.

Government officials look to the compliance professional and the corporate compliance function as the independent body and conscience of the organization. For healthcare professionals interested in compliance, the time to be proactive in identifying and mitigating risks throughout the healthcare enterprise is now.

Notes

1. An institutional compliance program can be either a voluntary undertaking by an institution to assure compliance with law or mandated as part of a corporate integrity program by the government (usually by the Department of Health and Human Services Office of Inspector General or the Department of Justice) as a condition of continuing participation in a government program after it has promised to correct the patterns of conduct that violate the law.
2. In a February 23, 2001, HHS press release, secretary Tommy G. Thompson stated, "These standards for privacy of individually protected health information are intended to ensure patients that the privacy of their medical records is secure and to ensure that this information is used appropriately. This administration is absolutely committed to achieving these goals." Available at http://www.hhs.gov/news.
3. Shalala, Donna. "Protecting Research Subjects-What Must Be Done." The New England Journal of Medicine 343, no. 11 (2000).
4. Office of Inspector General, Department of Health and Human Services. "Institutional Review Boards: A Time for Reform" (OEI-01-97-00193), June 1998, and "Protecting Human Research Subjects: Status of Recommendations" (OEI-01-97-00197), April 2000.

Odell Guyton *is corporate compliance officer for the University of Pennsylvania and the University of Pennsylvania Health System in Philadelphia. He can be reached at* guyton@pobox.upenn.edu.

Steps to Implementing a Compliance Program

If your organization is just starting a compliance program, here are some steps to keep in mind. Important activities to perform include:

- a legal audit of the organization
- identification of potentially unlawful or unethical conduct
- remediation of perceived difficulties
- drafting standards of conduct
- development and implementation of a mechanism to prospectively identify, investigate, and correct perceived compliance problems
- institution of a training program for management and employees

Next, design a mechanism to ensure that the program will be able to prospectively identify, investigate, and correct potentially unlawful or unethical practices. This includes conducting periodic internal audits, which typically involve regulatory and billing components. The audits are conducted according to protocol that specifies participation by an appropriate combination of internal personnel and outside consultants.

Understanding Risk

A compliance program is a voluntary process formally adopted by an entity's governance structure to adhere to its own internal practices and procedures and external regulation. The compliance process is, in turn, designed to proactively identify risk, correct known deficiencies, and create an effective mechanism to manage organizational risk. An effective compliance process, therefore, affirms an entity's formal commitment and obligation to uphold its own internal policies and procedures and to obey the external laws and regulations that govern it.

Today's aggressive business environment and evolving government enforcement initiatives create new challenges for all healthcare enterprises, private physician practices, and academic medical centers, regardless of their relative size or complexity. In this context, it is a well-accepted business principle that the voluntary adoption of an effective compliance program is an important step toward minimizing the adverse impact of mounting business risks.

An important benchmark for compliance programs are the seven criteria emphasized by the United States Sentencing Commission's promulgation of federal sentencing guidelines for organizations:

- create written policies and procedures and code of conduct
- designate a high-level manager for compliance
- establish a training program
- maintain consistent discipline for noncompliance
- maintain periodic auditing and monitoring
- implement corrective action procedures for noncompliance
- screen employees and contractors

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) rocked the auditing world when it issued its landmark report on internal control. The COSO principles recognized that as a result of the implementation of the federal sentencing guidelines, the concept of business risk should be considered broader than mere financial risk.

Business risk increases as the business environment changes. These environmental changes are driven by fierce competition, workplace pressure for increased productivity and reduced costs, powerful new technologies, and increased government scrutiny of how businesses conduct their affairs. Compliance programs face the same challenges.

Effective compliance programs are management processes that are strategically designed to address the broad spectrum of business risk. A voluntary compliance effort is part of an internal control system that must ensure efficient and effective operation, accurate financial reporting, and compliance with laws and regulations.

Benchmarking your compliance program and organizational management processes against the five COSO components of business risk is a good strategy. The components are:

- **financial risk**-inherent in safeguarding corporate assets
- **strategic risk**-inherent in achieving the stated goals and mission of the organization
- **operational risk**-related to maintaining the processes governing the daily operations of the organization
- **compliance risk**-associated with being noncompliant with laws and regulation
- **reputational risk**-associated with not maintaining a good public image

A compliance program will improve its effectiveness by proactively addressing these five components of risk. The compliance professional should also consider these strategic next steps for enhancement of a compliance program:

- ensure that everyone in the organization is concerned about risk
- understand the compliance officer's role in identifying and mitigating risk
- brainstorm ways for organizational leadership to either reduce or remove risk
- appreciate and understand that risk can be either eliminated, accepted, transferred, or mitigated-not ignored

COSO also advocates effective internal control environments that consist of five interrelated activities. They are:

- **control the environment**. This sets the tone of the organization from the top level of management and is the foundation of all other components of internal control
- **perform a risk assessment** to identify and analyze relevant risk to the organization
- **establish control activities** or policies and procedures that help ensure management directives are carried out
- **communicate**. Pertinent information must be identified and communicated up and downstream throughout the organization
- **monitor and assess** the quality of the compliance program's performance over time

Compliance Resource List

Article citation:
Guyton, Odell. "Compliance Programs: Beyond Billing and Coding." *Journal of AHIMA* 72, no.5 (2001): 49-53.
