HCCA

HEALTH CARE
COMPLIANCE
ASSOCIATION

COMPLIANCE TODAY

Volume Ten
Number Ten
October 2008
Published Monthly

Meet
Cathy Garrey,
Compliance and Quality Assurance Manager, McHenry County Mental Health Board
PAGE 14

Earn CEU credit
SEE INSERT

EXPLORING THE QUESTION: DOES THIS REALLY MAKE A COMPLIANCE PROGRAM "EFFECTIVE"?
PAGE 27

Feature Focus:
Coordinating external requests for information in the Compliance Office
PAGE 38

Connect with your Peers—Use HCCA's Compliance & Ethics Social Network
FIND OUT HOW ON PAGE 9

Coordinating external requests for information in the Compliance Office

By Cornelia M. Dorfschmid, PhD

Editor's note: Cornelia M. Dorfschmid is Executive Vice President with Strategic Management in Alexandria, VA. She may be reached by telephone at 703/683-9600, ext. 419 or by e-mail at cdorfschmid@strategicm.com.

The need for organization-wide strategies for coordination of requests for data, records, and patient information has taken higher priority in the Compliance Office these days. Despite of increased automation and software tools available to compliance officers, the handling of particular external requests for information warrants a fresh look.

A Compliance Office is faced with a multitude of coordination challenges. Examples include the coordination of compliance training efforts with other training initiatives across the organization, compliance investigations with legal counsel and the Human Resources department, and risk assessments related to regulatory requirements and quality-of-care issues. Facilitating the coordination and cooperation across departments is nothing new to an effective Compliance Office. It is part of the compliance officer's job. However, a new coordination challenge has moved to the forefront.

The Deficit Reduction Act of 2005 (DRA) strengthened Medicaid enforcement. A change in the enforcement landscape and Medicare reform brought a shift in the Center for Medicare & Medicaid Services (CMS) strategy to fight fraud and abuse. The Medicare Integrity Program and new national Medicaid Integrity Program are at the center of CMS's long-term antifraud and abuse strategy, which is focused on return on investment of enforcement efforts. In this context, new CMS contractors will request claims data and medical records, aggressively use data mining and statistical analysis to find payment errors, and have access to a powerful data warehouse containing vast amounts of information on providers and payment data. At the same time, boards of directors and external auditors are calling for increased transparency of how organization-wide risk management is conducted. Health care providers who have effective compliance programs will avoid meeting these demands one at a time. Instead, they will develop a solid response strategy to process external requests for information and data from government agencies, CMS contractors, oversight bodies, accreditation organizations, and independent auditors in a manner that coordinates efforts across departments and, as part of effective compliance risk management, leverages their own data analysis and review capabilities.

Request for information

Health care providers can receive a host of requests for data, medical records, billing information and claims data, the Disclosure of Financial Relationships Reports (DFRR) on physician arrangements, or policies and procedures from a myriad of requestors, including:

Medicare

- Zone Program Integrity Contractors (ZPIC) [formerly Program Safeguard Contractors (PSC)] that focus on billing fraud
- Medicare Administrative Contractors (MACs) [formerly Carriers and Fiscal Intermediaries] that process all types of Medicare claims
- Recovery Audit Contractors (RACs) that audit for Medicare claims, focus on billing errors and overpayments, and work on contingency basis
- Comprehensive Error Rate Testing (CERT) contractors that conduct random post-payment reviews of Medicare claims
- Medicare Quality Improvement Organizations (QIO) [successors of Peer Review Organizations (PRO)] that focus on quality of care

Medicaid/State

- Medicaid Integrity Contractors (MICs) that audit claims of providers of Medicaid services to identify overpayments
- Payment Error Rate Measurement (PERM) auditors that review Medicaid claims and beneficiary eligibility
- State Medicaid Fraud Control Units (MFCUs) that investigate state Medicaid fraud

- State OIG that fight Medicaid fraud and abuse (e.g., New York, Texas) and investigate and analyze claims – a growing trend to implement State OIG offices has been noted

General

- Department of Health and Human Services Office of Inspector General (OIG)
- Joint Commission [formerly Joint Commission on Accreditation of Healthcare Organizations (JCAHO)]

Requests are most commonly made by a "demand letter" via mail or fax, but may also involve e-mails, phone calls, and scheduled or unannounced site visits by an investigator or auditor. Subpoenas and search warrants are also a possibility. Unless there is coordination across the organization (based on written procedures) when these requests are made, unnecessary legal and compliance risks can arise or be aggravated. For example, a communication failure due to a non-timely response or a submission of a response letter that misses input, informational material, or prompt corrective action from some departments because they may remain unaware of the request or were inadequately informed, can pose legal, financial, and compliance risks. Such failures typically also involve a waste of resources, and even delay corrective action of detected or alleged systemic problems. When responding to an allegation or billing problem stated in the demand letter, being aggressively proactive is also important. Corrective measures should be put in place or at least be underway if substantial overpayments or lack of adequate controls are alleged. It is critical that "the left hand knows what the right hand is doing" to be proactive.

Taking responsibility to master the challenge

Two types of coordination challenges are associated with external requests for information: (1) the communication and handling of the incoming request, and (2) the coordination of the response and appropriate corrective action. The Compliance Office may want to take the lead in facing the coordination challenge.

A critical success factor in mastering the communication challenges is to engage various departments and assign responsibility, especially in larger health systems. Health care providers may consider the following:

- Designate an initial coordination response team (ICRT) with members of the senior leadership. The Chief Financial Officer (CFO), Legal Counsel (LC), Chief Operating Officer (COO), Chief Information Officer (CIO), and Compliance Officer (CO) should be considered as members of the ICRT.
- Ensure that the ICRT takes responsibility for coordinating the processing the external requests. Their responsibility is to notify each other when they become aware of an external request and ensure a concerted effort.
- Assign responsibility for maintaining a central tracking system, and
- Educate employees about requestors and the proper reporting of requests up the chain or to ICRT members.

Auditing & monitoring

The Compliance Office is a logical choice for taking on the responsibility of logging requests and responses. Alternatively, the Legal department may take on the task. As a quality assurance measure, the Internal Audit department and/or Compliance Office should periodically audit the request handling process and provide the executive-level Compliance Committee with a report on the major external requests and request-processing statistics (e.g., turnaround time and outcome, appeals involved, monetary impact, facilities affected, etc).

Getting Started. The Compliance Office that leads the charge of coordination may want to consider the following to get organized:

1. Develop a policy and procedure on coordinating, communicating, and handling requests for information from government entities and external organizations. The policy includes the role of an ICRT or similar task unit and is approved by the executive Compliance Committee.
2. Flowchart the process to illustrate clearly how a request and related documents are to be routed. Include regular status updates on the requests.
3. Make an inventory of current requests in process and categorize them, if not already done.
4. Develop a communication and training strategy to make employees aware of how to report any incoming requests for information and educate them on the new policy and procedure. Educate employees on the common types of requests with examples, the role of the ICRT, new types of contractors and sources of requests, and the basic reporting expected of them. Incorporate this effort into the compliance training program.
5. Dedicate staff in the Compliance Office to maintain a request tracking and logging system in accordance with a written procedure.
6. Implement an electronic request tracking system that can be easily maintained long-term. Categorize the requests into routine and non-routine and severity of potential problems, payment errors, or control weaknesses.
7. Use software that includes a database (e.g., a Microsoft Access

Continued on page 41

database and Excel worksheet; off-the-shelf vendor software application; a Web application that allows for tracking of compliance incidents/events; document management software that logs documents and assigns responsibilities for follow-up).

Discuss with the Information Technology (IT) department the options for a implementing a request tracking system that fits the organization's needs, configuration, and update issues. Include the possibility of integrating the requested correspondence files as electronic attachments. Explore how to implement secure access controls.

Review major data fields carefully when organizing the request tracking system. Activities, dates, documents, and responsibilities typically need to be logged in some type of field. Fields that hyperlink or electronically reference the main requestor documents and final response documents (e.g., demand letter by the government agency, provider's response correspondence) would be helpful.

Consider keeping all correspondence documents electronically. For example, scan all paper documents into Adobe PDF files (or similar format) and maintain these as electronic document attachments in the database of the request tracking system or in a dedicated drive on the network. Maintain version control between draft documents and final documents.

The data fields in a robust request tracking system should capture data, such as the date of initial request, requestor name and contact information, and any response due dates. The system should also log who at the provider was first contacted and which department and person is assigned to lead the effort to prepare the response. A date field to capture the day the ICRT was alerted and a data field for ICRT action taken may be helpful. In addition, fields that organize dates and documents related to the correspondence with the requestor (e.g., demand letter, response letter(s), appeal, etc.) help organize the tracking. Finally, data fields that capture internal actions taken, final outcome, closure date, and whether attorney-client privilege is applicable, may be needed. ■

Resources

CERT is a federally mandated program-integrity activity established by CMS to monitor and report the accuracy of Medicare fee-for-service (FFS) payments to physicians and non-physician practitioners. CERT contractors use CERT program information to determine which services are experiencing high error rates. See http://www.cms.hhs.gov/CERT/

DFRR (Disclosure of Financial Relationships Reports) are used by HHS as part of a "strategic and implementing plan." DFRR are meant to address certain issues relating to physician investment in specialty hospitals. HHS also stated that it would require all hospitals to provide information on a periodic basis concerning their investment and compensation relationships with physicians pursuant to 42 CFR §411.361. See http://www.cms.hhs.gov/PhysicianSelfReferral/05b_Disclosure.asp

MACs (Medicare Administrative Contractors). CMS is in the process of replacing current contracting authority with MACs to administer the Medicare Part A and Part B FFS programs. MACs will also take on payment error review functions previously carried out by Quality Improvement Organizations (QIOs). See http://www.cms.hhs.gov/MedicareContractingReform/ and http://www.cms.hhs.gov/AcuteInpatientPPS/downloads/InpatientReviewFactSheet.pdf

PERM (Payment Error Rate Measurement) auditors operate in a three-part sequence: sampling, collecting, and reviewing FFS and managed care Medicaid claims from providers in each state. Each state only participates in PERM once every 3 years. See http://www.cms.hhs.gov/PERM/ and http://www.cms.hhs.gov/PERM/Downloads/StatesSelectedForPERM.pdf

RACs (Recovery Audit Contractors) are a demonstration program and strategy begun by CMS to identify overpayments and underpayments to Medicare in New York, Massachusetts, Florida, South Carolina, and California. The RAC Program is being expanded to a 50-state permanent program. By 2010, CMS plans to have 4 RACs in place, each responsible for approximately one quarter of the country. See http://www.cms.hhs.gov/RAC/ and http://www.cms.hhs.gov/RAC/10_ExpansionStrategy.asp