

HCCA

COMPLIANCE TODAY

Volume Thirteen
Number Nine
September 2011
Published Monthly



HEALTH CARE
COMPLIANCE
ASSOCIATION



Meet

**Audrey Andrews, Senior
Vice President and Chief
Compliance Officer
of Tenet Healthcare
Corporation**

PAGE 14

Feature Focus:

**Reimbursement changes
under health care reform:
Are you prepared?**

PAGE 30

Earn CEU Credit

WWW.HCCA-INFO.ORG/QUIZ—SEE PAGE 39

**Security of
mobile devices in
health care**

PAGE 20



Record release compliance: The challenge accelerates

By Jan McDavid

Editor's note: Jan McDavid is Chief Compliance Officer and General Counsel at HealthPort in Alpharetta, Georgia. She may be contacted by e-mail at Jan.McDavid@HealthPort.com.

In 2010, more stringent Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security rules under the Health Information Technology for Economic and Clinical Health Act (HITECH) provision of the American Recovery and Reinvestment Act (ARRA) brought to light a misunderstood and often unknown process within health care: the release of medical records, better known as Release of Information (ROI). For years, Health Information Management (HIM) departments have been responsible for managing this elusive but critical function in health care. HITECH's updates to HIPAA made the process more structured and accountable.

And, as the process undergoes greater scrutiny, the challenge to consistently deliver timely ROI services at a low cost is accelerated. This article explains the ROI process and describes how industry forces, such as HIPAA, recovery audits, and meaningful use have made ROI an important topic for the Compliance table.

Release of information: What's the risk?

ROI is an important process, one that compliance officers must completely understand. Many may expect that somebody places a reasonable request for a patient's health information and a clerical worker in Medical Records simply makes a photocopy and forwards it on. Nothing could be further from the truth.

The actual ROI process is a highly structured, multi-step procedure designed to protect the information, the patient, and the institution. Recent changes make ROI more demanding, more important, and more expensive; however, the changes were imperative for compliance.

The dichotomy of increasing costs to remain compliant versus the trend to decrease costs in every health care institution requires a balancing act. Recovery audits have exponentially increased the number of information releases that are required, and the

penalties for improper or illegal release have increased as well. Finally, there are evolving rules for notifying the appropriate governmental agencies as well as the patients/individuals involved.

Business associates also in the mix

Another change that has impacted the ROI process is the inclusion of business associates (BA) into the HIPAA compliance mix. Business associate changes, effective in February 2010, were intended to ensure compliance throughout the chain of information movement. A business associate is anyone who works with or provides services to the covered entity involving the use or disclosure of PHI.

Rules apply to both the storage and transmission of paper and electronic versions of unsecured protected health information (PHI). The term "unsecured" is key. If electronic information is encrypted both while stored and transmitted, then it is deemed secured and not subject to penalty if breached.

Further, BAs are now subject to the privacy provisions of HIPAA to the same extent as the covered entity. Prior to February 2010, BAs were required to comply only with contractual obligations; now, they are compelled to adhere to all requirements of the HIPAA Privacy Rule, including the need to have

a privacy policy and appoint a privacy officer. The growing importance of compliance as well as an increased cost structure must be borne.

Recovery audits increase ROI volumes

The proliferation of audits is a second major health care initiative that impacts ROI. Health care providers have always been subject to some level of audit, but the Medicare Recovery Audit Contractor (RAC) program has sparked a major increase in the number and type of audits.

The goal of the audits is to mitigate fraud, abuse, and waste. Medicare uses contractors to do the audits. They are compensated based on a percentage of the monies that they re-coup from providers. This creates a “bounty hunter” mentality, which increases the aggressiveness of the audits. In 2010, \$1.7 billion worth of claims were audited, and \$86 million, or 5.05%, of the payout was recovered.¹

With thinning margins, most health care entities are hard pressed to lose more than 5% of their Medicare revenue stream. Worse, 2010 was just the buildup year for RAC audits, as they are expected to continue to increase. The apparent success of Medicare’s

audit programs has sparked other payers to take up the charge and start their own contractor-based audit programs. The Medicaid audit program was scheduled to start April 1, 2011, but it has been delayed to finalize rules. It will not likely start before January 1, 2012, but it is coming. Commercial payers hoping to recover payouts and help their bottom line have joined the fray.

“Having records available electronically is thought to be a magic bullet in expediting the ROI process. EHRs do relieve the ROI workload and cost slightly, but they also may heighten the risk of a breach.”

The point is that all this activity has greatly increased the number of requests for information that need to be managed and monitored for compliance. Compliance risk is mitigated with the use of a centralized audit management strategy and supporting audit tracking system. The centralized audit strategy has emerged as an industry best practice.

Meaningful use stimulus dollars and ROI

The government is trying to encourage providers to move to

electronic health records (EHRs). In an effort to define the effectiveness of EHRs, the government is certifying them and trying to ensure that the technology is used in a way that is “meaningful.” This meaningful use (MU) requirement, if fulfilled and attested to, will pay a bonus to the provider. Providers can choose to not pursue the MU program and not receive the bonus dollars but, if they do not demonstrate MU

in five years, they will be penalized by a reduction in Medicare reimbursements. The Phase One MU criteria have 25 components, five of which require the release of information to the patient or to another physician. It must be done electronically and in very short time frames (3-4 days). It must also originate from a certified EHR, to the extent the information exists there.

Having records available electronically is thought to be a magic bullet in expediting the ROI process. EHRs do relieve the ROI workload and cost slightly, but they also may heighten the risk of a compliance breach.

Releasing copies of medical records is a complex process consisting of highly regulated steps, only some of which are automated with an EHR. The process

Continued on page 52

has become increasingly labor intensive for HIM departments, diverting staff time from daily responsibilities to the administrative burden of managing all these record requests.

The most labor-intensive part of ROI involves a thorough review of each piece of documentation to make sure that no PHI is released without proper authorization. The fear is that many of the human checks and balances inherent in the process are eliminated in a completely electronic environment.

The logical inference with EHRs is that they afford greater user access to information, and they do. This increased access can help expedite processes and improve patient care. The potential downside of electronic record sharing is a much greater risk of a data breach. The compliance and security officers must be particularly vigilant in this brave new world and implement stronger disclosure and security practices to safeguard this information.

The final word on ROI

ROI's complexity is growing. The potential for breach is widening, and the need exists for tightening guidelines for security. The compliance officer must ensure that every HIM professional is knowledgeable about the privacy regulations of each medical condition, because the rules for all diagnoses

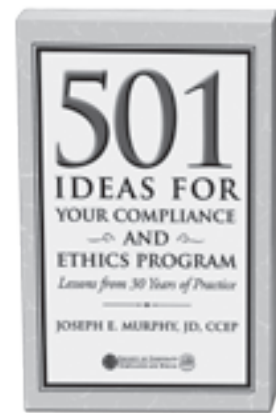
are not the same. To complicate matters, the regulatory requirements vary from state to state. In the case of state versus federal regulations, the most stringent regulation applies.

All of this is raising the cost structure for providers. The need for increased legal fees, software purchases, and encryption capabilities are small compared to the human capital required to be in compliance. And because the average reimbursement received from a record request is less than \$50, providers should not assume they can recoup the cost of compliance.

Finally, the negative effects of a breach due to improper record release must be weighed. Not only are fines and penalties involved, but breaches also impact a provider's community reputation. Having high-quality compliance staff, partners, policies, and procedures is a must in today's world. The need is only going to increase. ■

1. American Hospital Association: Exploring the Impact of the RAC Program on Hospitals Nationwide: Results of AHA RACTrac Survey, 4th Quarter 2010. February 24, 2011. Available at <http://www.aha.org/aha/content/2011/pdf/Q4ractracresults.pdf>

501 Ideas for Your Compliance and Ethics Program



Jump-start your program with SCCE's best-selling idea guide! Author Joe Murphy has spent his career collecting great ideas for building an effective compliance and ethics program. These practical tips can have an immediate, lasting impact on your organization's program.

Visit the HCCA store at www.hcca-info.org, or call 888-580-8373.