Fraud Management: a $100 Billion Bonus from Health IT?

Save to myBoK

by Linda Kloss, RHIA, CAE, chief executive officer

The financial losses from healthcare fraud in the US are staggering...and growing. Fraud was estimated to be between 3 and 10 percent of total health expenditures in 2003, or $51 to $170 billion, according to the National Health Care Anti-Fraud Association. Whether an interconnected health IT network would help reduce fraud was one of the questions addressed in groundbreaking research from AHIMA's Foundation of Research and Education.

Funded by the Office of the National Coordinator for Health Information Technology, the two-part study examined the potential for properly deployed health IT to improve the effectiveness of fraud management. Fraud management, defined as the prevention, detection, and prosecution of healthcare fraud, is a current focus of payers and law enforcement. The study concluded that health IT could give a major and critical boost to the effectiveness of current efforts, and the industry needs to get behind this initiative. Fraud management must be designed into health technologies, not added as an afterthought.

HIM professionals must think and work beyond compliance to use IT to prevent and detect fraud and ensure that there is a proper record for fraud prosecution when necessary.

Automated Coding and Fraud Management

The first part of the fraud and IT research examined automated coding software as an evolving technology. In "Fighting Fraud, Automatically," Jennifer Hornung Garvin, Valerie Watzlaf, and Sohrab Moeini describe automated coding software tools and the solutions that offer the greatest potential for fraud management. Artificial neural networks, rules engines, and pattern recognition databases have the potential to detect and prevent errors, thereby improving the accuracy of coding. Effective deployment requires sound work processes for documentation, coding, and revenue cycle management to strengthen the effect of automated coding software.

Revenue cycle management is the subject of other new FORE research, highlighted in "Benchmarking RCM." Researchers Amataykul and Work present benchmarks for effective revenue management and explore how technology, competent staff, and effective workflow improve HIM's contribution.

In "Following the Digital Trail," Gina Rollins reports on the necessity of well-designed audit and record verification tools in EHRs.

An Emerging HIM Role

The second part of AHIMA's anti-fraud study considered guiding principles of IT-aided fraud management and the macroeconomic impact of the transition from today's fragmented health IT system to an interconnected system. In "Fraud Control: New Tools, New Potential," Susan Hanson and Bonnie Cassidy spotlight the guiding principles developed by a national panel of experts. Read them carefully, as most are grounded in HIM practice. Note also the economic model that cautions against EHR adoption that stalls before achieving interoperability. The payback comes when our health system is interconnected, which must remain our goal.

The healthcare industry is in a strikingly similar position to that of the financial services industry 15 years ago. At that time, the banking industry began its transformation from paper to a sophisticated electronic environment. With a well thought-out vision and strategy, banking addressed the inefficiencies of paper and invested heavily in an IT infrastructure. Credit card fraud, estimated today to be less than 7 cents out of every 100 dollars, is widely perceived as a major problem. However, healthcare fraud is 100 times more costly! We have an opportunity and an obligation to help mitigate this unconscionable waste.

Article citation:
Kloss, Linda L. "Fraud Management: a $100 Billion Bonus from Health IT?" *Journal of AHIMA* 77, no.3 (March 2006): 23.