Fraud Control: New Tools, New Potential

Save to myBoK

by Susan P. Hanson, MBA, RHIA, FAHIMA, and Bonnie S. Cassidy, MPA, RHIA, FAHIMA, FHIMSS

With the right planning, health IT and nationwide health data exchange can deter healthcare fraud.

Fraud is a significant drain on the US healthcare system. The National Health Care Anti-Fraud Association estimates that 3 percent of the nation's annual healthcare outlay--$51 billion--was lost to outright fraud in calendar year 2003.[1] Other estimates by government and law enforcement agencies place the loss as high as 10 percent of annual expenditure, or $170 billion.[2] Healthcare fraud is a serious and growing crime nationwide, linked directly to the nation's increasing healthcare outlay.

Fraud is a moving target, shifting to new and more sophisticated schemes to mask aberrant behavior. For this reason, fraud control must be highly dynamic. Fraud management is made all the more imperative by federal efforts to promote a nationwide health information network (NHIN) that would link health data among providers and payers across the country. This prospect of highly mobile data--good for improving care and operational efficiencies--creates new challenges for fraud management. It also creates new potential.

In June 2005 the Office of the National Coordinator for Health Information Technology contracted with AHIMA's Foundation of Research and Education to conduct research assessing the potential of health IT to expand or enhance healthcare anti-fraud activities. The project's primary objective was to identify best practices that would enhance the capabilities of a nationwide interoperable health IT infrastructure to assist in healthcare fraud prevention, detection, and prosecution. (For more information on the contract and the resulting study, see "Background on the Report", below.)

The field-based research was directed at emerging and rapidly evolving technology and policy. It identified tremendous potential to reduce healthcare fraud and achieve substantial financial benefits through an NHIN and the interoperable electronic health records that would comprise it.

The Healthcare Fraud Problem

Fraud in healthcare is defined independently by a number of legal authorities, but all definitions share common elements: a false representation of fact or a failure to disclose a fact that is material to a healthcare transaction, along with some damage to another party that reasonably relies on the misrepresentation or failure to disclose.

Only a small percentage of the estimated 4 billion healthcare claims submitted each year are fraudulent. Taken in total, however, the resulting cost is high, and the scope of activity is wide. Fraud takes many different forms, such as incorrect reporting of diagnoses or procedures to maximize payments, fraudulent diagnosis, and billing for services not rendered. Examples include:

- Claims for phantom procedures
- Claims for visits that never took place
- Claims submitted under the guise of a falsified company using stolen or purchased provider and patient information
- Fabricated claims from nonexistent clinics
- Claims for durable medical equipment that was never received
- Providers who pay healthy citizens to make unnecessary visits
- Claims for unnecessary surgical procedures
- Payment for services for claims with medical necessity certificates signed by a provider for a referral kickback
- Nonprofessionals masquerading as healthcare professionals and delivering services without proper licenses
- Claims for services more expensive than those actually provided

- Multiple prescriptions for controlled substances obtained by patients who doctor-shop or bounce from one doctor to another
- Patient claims that nonmedical procedures were medically justified[3]

Fraud has experienced an explosive growth in some regions of the country--south Florida and Los Angeles are prime examples. It has become a career path of choice for criminals looking to reduce risk while increasing returns. Entrepreneurial criminals are abandoning drug trafficking or more dangerous activities to enter the safe and lucrative arena of healthcare fraud.[4,5]

It is not surprising that criminals are drawn to healthcare fraud. The Centers for Medicare and Medicaid Services project national health expenditures to reach $3.6 trillion in 2014, growing at an average annual rate of 7 percent from 2003 to 2014. One of the most significant impacts is the new Medicare Part D prescription drug benefit, which took effect in January of this year.[6]

Strengthening Fraud Control through Health IT

Technology can play a critical role in detecting fraud and abuse, and it can help enhance fraud management programs. While technology cannot eliminate the fraud problem, it can significantly minimize fraud and abuse and ultimately reduce healthcare fraud losses. The use of advanced analytics software built into an NHIN will be critical to fraud loss reduction. (For more on the fraud management potential of coding applications, see the article "Fighting Fraud, Automatically" (Garvin et al., *Journal of AHIMA* 77, no.3 [2006]:32-36).)

To maximize fraud control, information available via an NHIN must comply with all federal and state laws. The federal government continues to expand its initiatives to uncover healthcare fraud, waste, and abuse. It is important that healthcare organizations have an effective compliance program in place. It is particularly important that they develop corporate cultures that foster ethical behavior. Many healthcare organizations are doing so through the adoption of corporate compliance programs.

Further, a nationally accepted definition of the legal health record will be a crucial component in combating fraud. Currently there is no single definition of the legal health record; state laws and regulations differ regarding record format, content, and retention. In some states, electronic formats are not permitted. A national standard for the legal health record would enable the use of advanced analytics software on an NHIN to prevent, detect, and prosecute fraud. There is also no definition that encompasses the more complex electronic environment and various hybrid situations between paper and electronic records.

The interoperability of EHRs offers major improvements in fraud management efforts. Interoperability between payers and providers will enable validation of a clinical encounter between the provider and the patient. When claims data can be electronically linked to encounter data, payers can validate claims prior to payment. Thus interoperable EHRs will help transform fraud management from a "pay and chase" model to a "validate and pay" model, powered by advanced analytic software.

NHIN Benefits in Stages

An NHIN's greatest potential for deterring fraud will come in its advanced implementation, with fully interoperable EHRs and integrated advanced fraud-control tools. The research envisioned four states through which the NHIN will evolve:

- **The status quo**, as it is anticipated to be in 2006 after implementation of the Medicare Part D prescription benefit. In this state, there is no NHIN. Some EHRs and electronic transactions such as e-prescribing exist, but with the exception of claims and prescription databases, there is little aggregate clinical data and no interoperability.
- **Early NHIN.** In this state, electronic clinical transactions such as laboratory results and e-prescribing become widespread. EHR adoption increases, but there remains little EHR interoperability among providers.
- **Intermediate NHIN.** This state features interoperability with intelligent coding tools that search for fraud. A record locator system facilitates the exchange of clinical records among providers. Clinical vocabularies are in widespread use, ICD-10 has been implemented, and intelligent coding tools are used for claims generation.
- **Advanced NHIN.** Advanced analytics exist in this state. Interoperability enables the aggregation of rich clinical and financial databases to which advanced analytic techniques are applied to detect patterns of fraud.

Moving to interoperability in the intermediate state may provide the most dramatic improvement in fraud net cost and benefit. There may be substantial savings in fraud-related expenditures that are possible from a move to this state that are not realized in the status quo and early NHIN states.

Next Steps

Fraud harms everyone in healthcare. The principles presented in "Guiding Principles", below, and detailed in the report offer a starting point for efforts necessary to further prevent, detect, and prosecute healthcare fraud. At a minimum, the next steps for consideration include:

- Defining a single definition of the legal health record across the country
- Defining the infrastructure components that must support the legal record for both patient care and as admissible evidence in fraud management
- Defining the standards for EHR process and data standards that both facilitate fraud management and prevent abusive and fraudulent behavior
- Adopting national metrics for healthcare fraud management to systematically gauge and reduce healthcare fraud
- Raising awareness of the importance of coordinated fraud management across all stakeholders
- Continuously revising and updating the NHIN economic model presented here

HIM professionals will have a critical role in healthcare fraud control. As EHRs are implemented and become interoperable, HIM professionals will be responsible for ensuring that electronic health information is managed to enable effective fraud management. For more on the HIM role, see "A Call to Action for HIM Professionals," below.

Background on the Report

This article is excerpted from "Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities," a report prepared by AHIMA's Foundation of Research and Education (FORE) under contract with the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology.

The research behind the finds reported here consisted of five components:

- **Executive committee.** FORE convened an executive committee to identify the best opportunities to strengthen the fraud management capability of a nationwide interoperable health IT infrastructure. The committee consisted of 22 cross-industry experts from provider, payer, IT, fraud investigative, financial, and government organizations. The composition of the committee was designed to bring together an expert panel reflecting a diversity of roles and perspectives.
- **Literature review.** Findings from the review were used to develop the data collection tool for the site visits and interviews and to formulate and validate the discussions associated with the development of the guiding principles and recommendations.
- **Site visits and interviews.** Site visits, in-person interviews, and telephone interviews were conducted using a structured data collection instrument. Telephone and in-person interviews were conducted with approximately 117 individuals representing both the public and private sectors.
- **Executive committee work groups.** Five working committees of the executive committee were established to develop guiding principles and recommendations related to the following five core areas of focus: guiding principles, law enforcement and prosecution, fraud management, information technology infrastructure and implementation, and economic impact.
- **Economic model.** The principal research question for the economic framework asked, "What are the expected fraud- and nonfraud-related costs and benefits associated with developing and implementing an NHIN with interoperable EHRs" The four models developed in the research are summarized in this article under the heading "Strengthening Fraud Control through Health IT"; they are discussed in detail in the report.

The full report includes further background on the study methodology and greater detail on fraud costs and estimated benefits. The economic model is presented in greater depth. The full report may be read online at www.ahima.org/fore/fraudrpt.asp.

Guiding Principles

The following principles and recommendations offer a road map to ensure that design of an NHIN deters fraud and enables cost-saving anti-fraud activities. They are based on a solid understanding of the vulnerabilities of the healthcare system to individuals with the intent to defraud and the opportunities that well-designed health IT offers. They are intended to guide policy makers and to support the needs of the vast majority of service providers who are striving to comply with laws and requirements that affect billing and reimbursement.

1. While many of the recommendations cannot currently be implemented, they identify the future technology, capability, and capacity that will be needed.
2. NHIN policies, procedures, and standards must proactively prevent, detect, and support prosecution of healthcare fraud rather than be neutral to it.
3. EHRs and information available through the NHIN must fully comply with applicable federal and state laws and meet the requirements for reliability and admissibility of evidence.
4. A standard minimum definition of a legal health record must be adopted for EHRs.
5. Comprehensive healthcare fraud management programs must enable rather than inhibit nationwide EHR adoption.
6. Healthcare fraud management is the responsibility of all healthcare stakeholders.
7. Increased consumer awareness of healthcare fraud and the role health IT and EHRs play in its reduction can improve the effectiveness of healthcare fraud management programs.
8. EHR standards must define requirements to promote fraud management and minimize opportunities for fraud and abuse, consistent with the use of EHRs for patient care.
9. Standardized reference terminology and up-to-date classification systems that facilitate the automation of clinical coding are essential to the adoption of interoperable EHRs and the associated IT-enabled healthcare fraud management programs.
10. Fraud management programs and advanced analytics software must be fully integrated into interoperable EHRs and the NHIN to achieve the full expected economic benefits of fraud control.
11. Data required from the NHIN for monitoring fraud and abuse must be derived from its operations and not require additional data transactions.

A Call to Action for HIM Professionals: Electronic Fraud Management Programs Will Benefit from HIM Participation

HIM professionals can play a significant role in building healthcare fraud management into an NHIN. Designing a comprehensive anti-fraud component should not be an afterthought to interoperability. David Brailer, MD, PhD, national coordinator for health information technology, raised this point to the profession at the AHIMA national convention in October 2005. He expressed the need to use the guiding principles presented here in the design and implementation of the NHIN infrastructure prototype. He noted the need for ongoing review of the principles as work progresses.

Education, Legal Records

HIM professionals can begin their fraud management efforts by spreading the word. An NHIN with anti-fraud components has the potential to identify emerging fraud schemes prior to payment and to be a powerful weapon against fraud. It will have a positive effect on the quality of patient care and patient safety.

For example, one fraud scheme reported in the research involved billing for expensive wheelchairs and wheelchair accessories that were never purchased or delivered. The fraud wasn't discovered until patients needing wheelchairs found they were on record as having received one already. They were thus ineligible for a new wheelchair for another five years. That scheme paid millions of dollars to criminals and left elderly patients struggling to prove they were the victims of identity theft.

The need for a universal definition of the legal electronic health record is an area particularly suited to HIM expertise. The guidelines, policies, and procedures for the paper medical record must be evaluated and revised or updated to meet the requirements for the legal electronic counterpart. Everything that HIM professionals look for in the paper record must be addressed in the EHR as we define the digital business record.

HIM professionals have always certified maintenance of the paper health record for admissibility as evidence in a fraud case. The same issues must be addressed for an EHR's admissibility in a court of law. HIM experience lends itself to certifying the electronic management of health information.

Ways to Get Involved

Standards, metrics, interoperable EHRs, and fraud management functionality built into an NHIN are all critical to the effective management of healthcare fraud. HIM professionals can take leadership roles in their organizations, promoting the inclusion of healthcare fraud management principles in EHRs, regional data exchanges, and an NHIN. They can start by:

- Participating and leading the development of health fraud management programs
- Participating in work to incorporate standards, procedures, and prototypes that facilitate nationwide fraud management as part of an NHIN infrastructure
- Working on the national effort to develop metrics for fraud management, measures necessary to systematically gauge and reduce healthcare fraud
- Leading the effort to define the minimum components of the legal electronic health record that can be adopted nationally
- Helping define the standards for EHR process and data standards that both facilitate fraud management and prevent abusive and fraudulent behaviors
- Assisting in the development of NHIN IT infrastructure requirements to match or link electronic clinical documentation with corresponding claims
- Promoting the adoption of uniform rules, regulations, and guidelines for standardized reference terminology and up-to-date classification systems across the country

These efforts will help shift fraud management programs from the current "pay and chase" approach to the proactive prevention of fraudulent claims prior to payment. HIM professionals can demonstrate that e-HIM® professionals working in the development and expansion of healthcare fraud management programs will result in effective healthcare fraud management and provide a real chance to solve a $51 billion problem.

Notes

1. National Health Care Anti-Fraud Association. "Healthcare Fraud: A Serious and Costly Reality for All Americans." April 2005. Available online at www.nhcaa.org.
2. Ibid.
3. Blue Cross and Blue Shield Association. "Anti-Fraud: What the Blues Are Doing about It." Available online at www.bcbs.com/antifraud.
4. Freeh, Louis J., director, Federal Bureau of Investigation. Statement before the Special Committee on Aging, US Senate, Washington, DC, March 21, 1995.
5. Sparrow, Malcolm K. "Fraud Control in the Healthcare Industry: Assessing the State of the Art." National Institute of Justice: Research in Brief (December 1998). Available online at www.ncjrs.gov/pdffiles1/172841.pdf.
6. Centers for Medicare and Medicaid Services. "NHE Projections 2004-2014." Available online at http://new.cms.hhs.gov/NationalHealthExpendData/03_NationalHealth AccountsProjected.asp.

Susan P. Hanson *(s.hanson@terrastarconsulting.com) is president of TerraStar Consulting in Nashua, NH.* ***Bonnie S. Cassidy*** *(bsc1107@bellsouth.net) is president of Cassidy & Associates, based in Norcross, GA.*

Article citation:
Hanson, Susan P.; Cassidy, Bonnie S.. "Fraud Control: New Tools, New Potential" *Journal of AHIMA* 77, no.3 (March 2006): 24-30.