HealthManagement.org
The Journal
LEADERSHIP • CROSS-COLLABORATION • BEST PRACTICE
VOLUME 17 • ISSUE 2 • 2017 • € 22
ISSN = 1377-7629

HEALTHCARE EXECUTIVE ALLIANCE SPECIAL EDITION ON E-LEARNING

Money Talks

- COSTS, COSTS, COSTS! WHO PAYS IN HEALTHCARE?, *C. MCCAHAN*
- HOSPITAL FINANCE, *M. NOPPEN*
- TRANSFORMING COMMISSIONING TO DO MORE WITH LESS, *C. COTTON*
- MAKING AFFORDABLE HEALTHCARE PROFITABLE, *A. MIR*
- PRESENTING A CASE: FINANCING IT PROJECTS, *M. HASIB ET AL.*
- NATIONAL TELEHEALTH CAN SAVE MONEY AND IMPROVE HEALTH, *H.E. HENRIKSEN*
- FINANCE TECHNOLOGY BLOCKCHAIN IN HEALTHCARE IT SECURITY, *T. LAURENCE*
- FRAUD IN HEALTHCARE, *S. PECK & L. MCKENNA*

Fraud in Healthcare

A Worldwide Concern

The Global Health Care Anti-fraud Network (GHCAN) promotes partnerships and communications between international organisations in order to reduce and eliminate healthcare fraud around the world. *HealthManagement* spoke to representatives, Simon Peck (UK), and Leigh McKenna (USA) to find out more.

Simon Peck
Past Chair
Health Insurance Counter Fraud Group (HICFG)
Rickmansworth, UK

dr.simon.peck@gmail.com

@HICFG

hicfg.com

Leigh McKenna
Director of Government & Public Affairs
National Health Care Anti-Fraud Association (NHCAA)
Washington, DC
USA

lmckenna@nhcaa.org

@NHCAA

nhcaa.org

What is the range and scope of healthcare fraud?
Common healthcare fraud schemes include:

- Upcoding: billing for more expensive services or procedures than were actually provided or performed
- Charging for treatment not given
- Performing medically unnecessary services solely to generate insurance payments
- Misrepresenting non-covered treatments as medically necessary covered treatments to obtain insurance payments
- Falsifying diagnoses to justify tests, surgeries or other procedures that aren't medically necessary
- Unbundling, ie, billing each step of a procedure as if it were a separate procedure
- Accepting kickbacks for patient referrals
- Failing to provide necessary services prepaid under a health plan
- Billing a patient more than the co-pay amount for services that were prepaid or paid in full by the benefit plan under the terms of a managed care contract
- Double charging, often concealed in jargon
- Misrepresenting the type of treatment, for example doing cosmetic work and claiming it is medical treatment
- Specific types of fraud involving pharmaceuticals, for example charging for branded drugs and using simple generics, charging for more drug than was used and diversion of drugs into the black market, for example opiates or drugs of addiction
- Specific frauds involving pathology: one of the first major anti-fraud initiatives was by the Federal Bureau of Investigation (FBI) in the USA and called operation labscam, which involved many fraudulent practices by laboratories. For example the case reported here by the U.S. Department of Justice **justice.gov/archive/opa/pr/2001/January/002civ.htm**

Simon Peck (SP): There is a spectrum of behaviour, which we term fraud waste and abuse—all of which has at its heart taking money inappropriately out of the healthcare system. Fraud is a criminal offence (even though most cases are not prosecuted through the criminal system) and is the use of false statements, omission of information or abuse of a position of trust with the intention of making a gain. Waste is the deliberate consumption of resources for financial gain rather than for the benefit of patients, which includes providing unnecessary treatments or investigations. Fraud and waste can overlap. Abuse covers things like excessive and unreasonable billing.

Health fraud, waste and abuse is more often committed by healthcare providers than patients, although anyone in the system can be fraudulent. This includes patients, staff and people who are not actually working in healthcare at all, but who try to take money from the system. More serious but less common is organised criminal activity such as counterfeiting, or a recent multi-million pound scam, conducted electronically, which hit many UK-based insurers, and involved multiple bogus expatriate policies sending in fictitious bills for treatment.

Leigh McKenna (LM): While healthcare is in a state of perpetual change and evolution, fraud is seemingly a constant, complex crime that can manifest in countless ways. In the United States the sheer volume of healthcare claims and the data involved makes fraud detection a challenge. For instance, Medicare Parts A and B alone process 4.6 million claims per day. Fraud can be committed by anyone: physicians and other providers, employees with access to medical and claims records, enterprise crime organisations, and even patients. Detecting healthcare fraud often requires the knowledge and application of clinical best practices, as well as knowledge of medical terminology and specialised coding systems.

The perpetrators of some healthcare fraud schemes deliberately and callously place trusting patients at significant risk of injury or even death. There are cases where patients have been subjected to unnecessary or dangerous medical procedures simply because of greed. Patients may also unknowingly receive unapproved or experimental procedures or devices. Healthcare fraud is clearly not just a financial crime, and it is certainly

CHECKLIST

- ✓ Be aware of the risk of healthcare fraud and design it out where possible
- ✓ Where it cannot be designed out, minimise the opportunity and have robust systems of checks and audits
- ✓ Have senior management who understand and are committed to dealing with the problem

not victimless. With its complexity, the U.S. healthcare system can be susceptible to creative, nimble and aggressive perpetrators who have a knack for identifying weaknesses.

What is the scale of the problem? Is fraud becoming more sophisticated?

SP: In the UK we estimate fraud in the private sector to be about 5% of claims paid. In any environment, only a small number of people are fraudulent by nature—many more go along with the culture, and we have worked hard to raise awareness and try to send the message that such activity is unacceptable. There is no evidence that fraud has become more sophisticated in the UK. The response has, however, as we have sought to learn from our partners in the U.S. Insurers have become a lot more capable with the use of technology to highlight problems, professional investigators and other skills. We recognise that a successful response needs medical input and good legal advice as well as skilled investigators. The most important thing is to stop losses, and we always try to understand the root cause or weakness that has been exploited to prevent recurrence. The anti-cybercrime industry does this well, looking at the opportunities that were exploited when responding to a threat because closing the door to future losses may be the only thing that is possible.

The UK health insurance sector was the first industry in the UK to start comprehensive sharing of intelligence, including the names of fraudsters. This has enormously increased our capability and ended the problem where fraud in one area simply reinvents itself at a different insurer or payer.

LM: Fraud trends and schemes are constantly changing, developing, shifting, migrating and morphing, and the task for anti-fraud professionals to stay ahead of the threat is daunting. Some frauds are impressively sophisticated while others are remarkably absurd. And in many cases—such as with phantom providers—speed is the key. Someone who sets up a false storefront with the intention of filing false claims, will submit many claims, receive payment and abandon the property before investigators are able to intervene.

Some of the areas of healthcare that seem to be indicating the greatest uptick in or susceptibility to fraud include:

- Organised criminal enterprises (could invoke several types of schemes but seem to depend significantly on medical identify theft—theft of patient and provider identities)
- Infusion therapy
- Pain management (office-based opioid therapy)
- Pharmaceutical/drug diversion
- Durable medical equipment (involves significant medical identity theft)
- Behavioural health and community mental health centres
- Medical Identity Theft (Medical ID theft is often an element of a broader healthcare fraud scheme)
- Home healthcare
- Cardiology
- Ophthalmology
- Physical therapy and occupational therapy (medical necessity, spa vacations)
- Transportation (ambulatory)

> “HEALTH FRAUD WASTE AND ABUSE IS MORE OFTEN COMMITTED BY HEALTHCARE PROVIDERS THAN PATIENTS”

What do healthcare leaders and frontline clinicians need to be aware of?

SP: One of the main strands of an anti-fraud programme is creating an anti-fraud culture, which means raising awareness and mobilising the honest majority. The perception is that healthcare workers work only for the good of patients. This is undoubtedly the case for most of them, but the healthcare system also attracts fraudsters, criminals and charlatans. Awareness of the problem is the single biggest hurdle, and once this is in place, healthcare managers need to ensure that they have a robust programme to assess and minimise the risks, then put in place appropriate controls and checks, and have an enforcement regime or agency which is able to deal with the very complex issues which can arise.

Do governments and regulators have sufficient powers to combat fraud?

SP: In the UK the National Health Service (NHS) Protect Agency has extensive powers to tackle fraud and does

so using criminal prosecution. However, the regulatory system in the UK is not as effective as it should be. There are too many bodies, and they do not communicate well. Criminal prosecution is not suitable for all matters; the standard of proof is very high, it is very time-consuming and has very strict rules on evidence for example. Regulators have a very definite place in dealing with problems not suitable for the criminal courts. The UK needs an agency to oversee and coordinate the various healthcare regulators, which currently are not as effective as they should be.

LM: The laws and regulations currently in place in the United States are for the most part quite sufficient. In the 1990s there was discussion among federal and state officials, insurers and state insurance commissioners, of a federal immunity statute, for insurers sharing fraud-related information with other insurers. Unfortunately, the legislation that would have implemented these ideas was not enacted, but many states have since enacted their own state immunity statutes. NHCAA believes that we should remove unnecessary obstacles that inhibit fraud fighting efforts, and that providing protections for individuals and entities that share information and data concerning suspected healthcare fraud is reasonable and prudent.

What role does IT play in detecting potential fraud?

SP: Most payment systems are IT-based, and the most important thing is to build into the system appropriate controls, red flags and alerts to automatically identify suspicious transactions. Because most provider fraud is repeated there is an important role for IT in looking at patterns of conduct, which may be acceptable in an individual case but which if repeated are very unlikely to be genuine. IT is not the answer on its own. The basics need to be in place first, namely policies and procedures for financial controls, staff training and proper oversight.

Analytics are a useful addition to a mature entity that has the capability and understanding of the problem and is able to interpret the outputs and respond appropriately. In isolation they have very little if any value, and may actually be detrimental, as few managers want to see a problem they can neither control nor understand.

LM: IT plays an enormous role in detecting fraud. The USA's healthcare system hinges upon a staggering amount of data spread across the healthcare claim adjudication systems of numerous payers. Given the diversity of providers and payers and the complexity of the health care system—as well as the sheer volume of activity—the fraud prevention challenge is enormous.

It is more cost-effective to detect and prevent fraud before paying a fraudulent claim than to chase the lost dollars after the fact. The "pay and chase" model of combatting healthcare fraud is no longer tenable as the primary method of fighting this crime. The only way to detect emerging fraud patterns and schemes in a timely manner is to aggregate claims data as much as practicable and then to apply cutting-edge technology to the data to detect risks and emerging fraud trends. NHCAA supports efforts among its members, both public and private, to shift greater attention and resources to predictive modelling, real-time analytics and other data-intensive tools that will help detect fraud sooner and prevent it before it occurs.

However, data analytics is not a panacea. For instance, predictive analytics can generate leads for further inquiry and can help form the basis for the suspension of payments, but it has not been used as the sole basis for the suspension of payments by private health insurers without additional follow-up and corroboration.

Many of the data analysis and aggregation tools and systems being developed and brought to market are incredibly powerful and can produce potential leads at a pace that can quickly exceed what the finite investigative resources can handle. The need for "boots on the ground" is as great as ever. Technology professionals and data analysts will be in increasing demand as the use of prepayment technologies grows. And the leads and information developed by data analytics will continue to require, in many instances, skilled investigators and medical record reviewers with clinical backgrounds available to act on the information.

As we focus on the promise of technology, we mustn't overlook the vital need for smart, analytical, insightful, and committed fraud-fighting professionals. We must maintain a multi-pronged approach to fighting healthcare fraud that strikes a balance between technological resources and human resources.

What are the critical success factors for detecting fraud and recouping the money?

SP: In addition to the basics, professional investigation teams with access to clinical and legal support, clear contracts and strong management support. Key to recovering money is meticulous casework. It can be difficult for non-fraud trained management to understand the need to build a case methodically without making assumptions and collect the evidence and present it systematically. It is one thing to "know" that someone has committed a fraud, but to make a recovery this has to be proven.

LM: Focusing on "recouping" money is no longer the sole or primary function of an insurer's anti-fraud unit. The most advantageous goal, both monetarily and for patient safety, is to prevent fraud. Detecting it before claims are paid should be the next priority. There is no single solution. The landscape we are dealing with demands multi-faceted anti-fraud efforts. ■