

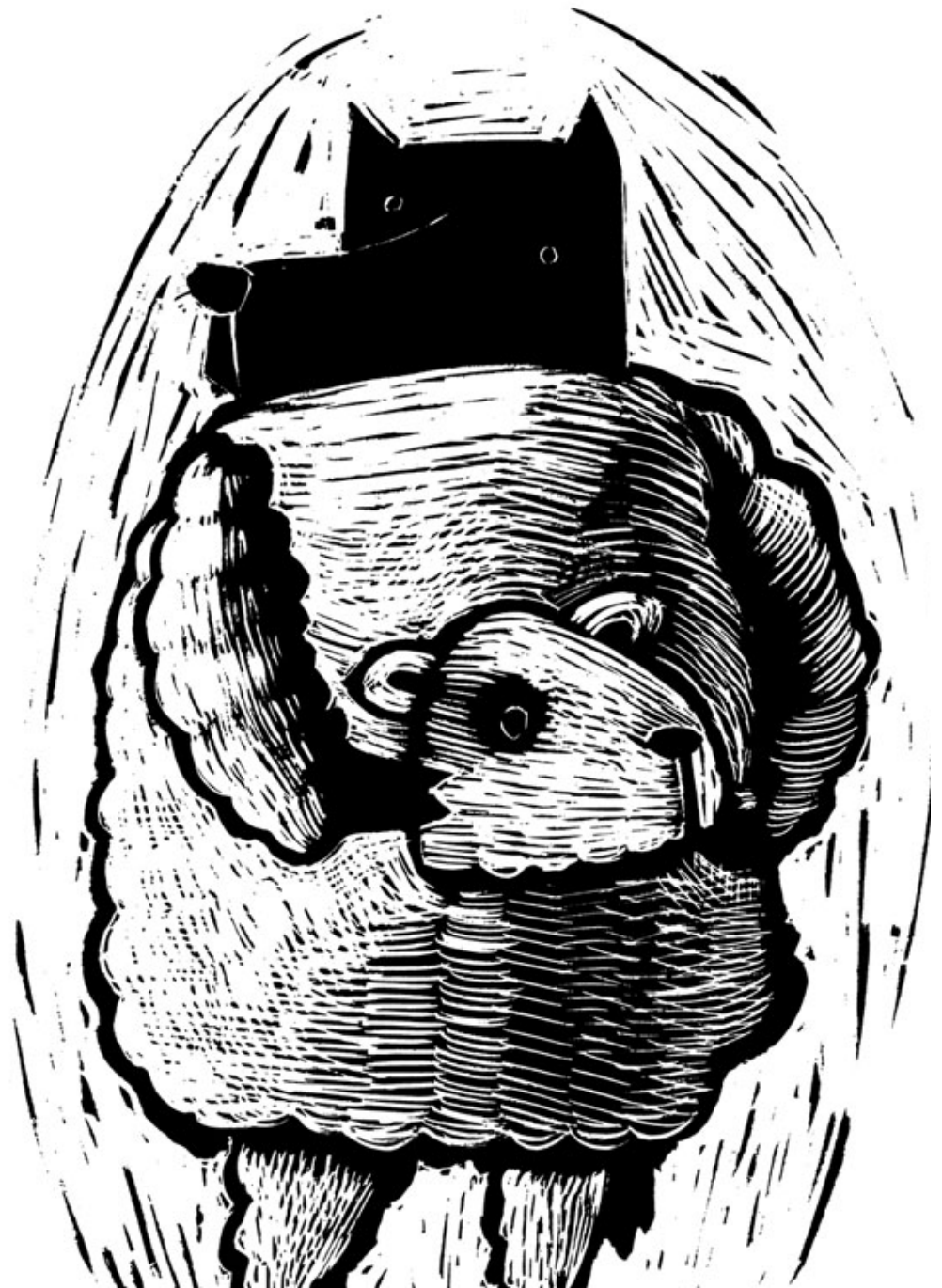


An Innocent Mistake or Intentional Deceit?

How ICD-10 is blurring the line in Healthcare Fraud Detection

October 2012

Whitepaper Series
Issue No. 7



ICD-10's impact will reach far beyond the October 2014 deadline. As providers and payors work through coding productivity drops, significant fluctuations in revenues, and operational impacts, they face another, longer lasting challenge—fraud. The core algorithms driving healthcare fraud detection are based on machine learning that identifies patterns related to the underlying code set. That is, they rely on programs that are continually refined based on new situations and circumstances, which ultimately increases performance and improves accuracy (Nilsson 2005). With the introduction of ICD-10's new coding language, those algorithms effectively become a blank slate thereby blurring the line between genuine coding mistakes and legitimate healthcare fraud.

Defining Healthcare Fraud

The National Healthcare Anti-Fraud Association (NHCAA)—the preeminent organization focused on fighting healthcare fraud—(<http://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-problem-of-health-care-fraud.aspx>) defines the most common kinds of fraud as:

- Billing for services that were never provided
- Billing for services that were more expensive than those actually provided
- Performing unnecessary services
- Misrepresenting treatments that were non-covered as medically necessary
- Providing false diagnoses
- Unbundling procedures so that they appear separate
- Overbilling a patient his or her co-pay
- Waiving a patient's co-pay while overbilling the insurance company
- Accepting kickbacks

(NHCAA 2012)

To report and ultimately prevent healthcare fraud, the NHCAA established and continues to build multiple programs. While some of these efforts—like anonymous reporting outlets for Medicare fraud—are equally applicable in ICD-9 and ICD-10, others

that are based on machine learning will lose their efficacy in a post ICD-10 environment. This is especially alarming given the centrality that data aggregation and analysis play in the overall approach to fraud detection. In a recently published NHCAA whitepaper, the organization highlighted the important role of analytics in combating healthcare fraud within a post-reform environment. “Clearly, 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 emerging fraud trends” (NHCAA 2010).

The New Language of ICD-10

Detecting healthcare fraud relies on complicated mathematical formulas that look for outliers across variables such as average dollars paid per patient, average number of visits, average paid per medical procedure, and average medical procedure per visit among other parameters. With the exception of kickbacks, most of these processes are driven by machine learning technologies that use the underlying lexical or natural language associated with claims data to identify trends and suspicious transactions. For example, if a provider averages six office visits per year while others in the area average three or a patient travels more than 250 miles for routine care, statistical interconnectedness and rule-based logic would flag these cases for investigation.

But with ICD-10, things change significantly. ICD-10 will at least temporarily handicap the capabilities of these automated detection algorithms by completely changing the coding language. In essence, most of the patterns that the machines “learned” over time will be wiped away leaving open opportunities for costly mistakes. It is estimated that it will take anywhere from 18 to 24 months for machines to regain the statistical capabilities that drive accurate fraud detection. This means that—despite ICD-10's overall benefits to reducing fraud in the long run—unethical organizations and individuals may be able to hide behind the complexity of the code set for two to three years before detection systems are fully operational and trustworthy. Conversely, honest

Payor Challenges

- Addressing the increased chance that genuine mistakes will be flagged as fraud
- Managing the greater likelihood that fraudulent behavior will slip through current detection algorithms
- Addressing operational and financial impacts related to an increase in the number of fraud investigations

individuals and organizations may face increased scrutiny and false accusations because of the heightened possibility that genuine mistakes will be flagged as fraud.

The Impact on Payors

For payors, ICD-10 poses a conundrum. On the one hand, outliers may simply be genuine mistakes. On the other hand, items may be flagged because of outdated or untried ICD-10 fraud detection algorithms. In either case, the payor wants to avoid making incorrect claims of fraud because investigations are costly and demanding. So while payors wait for the algorithms to “learn” the ICD-10 code set, they may be forced to lower fraud detection levels to avoid misinterpretations and artificially inflating fraud allegations. But this solution comes with a price. If payors lower their sensitivities, actual fraudulent claims may slip through the system costing the industry millions.

The Impact on Providers

Because of the increased likelihood that claims will be flagged as fraud following the conversion to ICD-10, providers face a real threat to their credibility. A provider’s credibility, which acts like a risk rating, helps payors determine which providers they will work with and influences the decision to put a provider on a pre-pay schedule. If genuine coding mistakes or new coding procedures are flagged as fraudulent because of incipient detection algorithms, a provider’s credibility and their overall standing will lower. Once lost, this credibility is hard to gain back.

Provider Challenges

- Maintaining credibility as mistakes are incorrectly identified and investigated as fraud
- Responding to an increased number of fraud allegations
- Driving optimal coding in ICD-10 while avoiding allegations of “up-coding”

Falling Short at The Front Line

The American Medical Association (AMA), whose members have launched a campaign against insurance company billing practices, blames errors in claims processing for an extra \$17 billion in 2011 administrative costs carried by physicians. According to the group, nearly 20 percent of the claims doctors get back from insurance companies have mistakes (AMA 2012).

To combat errors, the AMA recommends that insurers increase the timeliness of payments, increase the transparency of rules used to edit medical claims, and reverse the overall increasing trends in denials (AMA 2012). In addition, The Office of Inspector General (OIG) for the US department of Health and Human Services (HHS) created education resources for physicians summarizing the five main Federal fraud and abuse laws (U.S. Department of Health & Human Services 2012):

- False Claims Act
- Anti-Kickback Statute
- Stark Law
- Exclusion Statute
- Civil Monetary Penalties Law

This material provides tips on how physicians should comply with these laws in their relationships with payers (e.g., the Medicare and Medicaid programs), vendors (e.g., drug, biologic, and medical device companies), and fellow providers (e.g., hospitals, nursing homes, and physician colleagues).

“With the introduction of ICD-10’s new coding language, fraud detection algorithms effectively become a blank slate thereby blurring the line between genuine mistakes and legitimate fraud.”

But there is a gap. Both the AMA's recommendations and available physician education fall short of addressing ICD-10 related challenges:

- The recommended efforts outlined by the AMA are all undermined by ICD-10. Payors will take longer to process ICD-10 claims as they learn to adapt to new processes based on the increased specificity within the code set and work to ensure accurate fraud identification. Medical claim edits and rules will undergo a period of adjustment and fluctuation as algorithms and systems adapt. And denials will increase as providers and payors adjust to new coding requirements
- Existing education materials do not describe how laws will discern genuine versus intentional fraud after October 2014 leaving a large grey area open to interpretation. This undefined space will ultimately translate into increased administrative costs and burdens for providers and payors

Separating the Sheep from the Wolves

While the industry waits for existing fraud control processes to catch up with ICD-10, payors and providers need a solution that will augment existing algorithms to drive accurate and timely fraud detection. Newer technology is emerging that leverages big-data-based predictive analytics has the potential to address this transition period by providing faster machine learning as well as highly sensitive and specific fraud detection. These new advancements lay the foundation for different kinds of algorithms that rely less on the code information within claims data.

Decreasing dependence on a code-set for fraud detection could open doors for more sophisticated algorithms that combine leading approaches to unstructured text analysis with innovations in capturing, analyzing, and managing disparate data. This kind of innovation is made possible, in part, by ICD-10's greater specificity and larger code set. As providers are forced to define procedures and diagnosis at a more granular level, there is more data available. That data will drive greater visibility into patterns of behavior and better insights to more precisely identify fraud within a shorter timeframe.

For more information on Jvion, please e-mail us at contact@jvion.com or call us at 678.889.1842

“New technology is emerging that leverages big data concepts and predictive analytics to address gaps created by the lag in machine learning”

Works Cited

- AMA. AMA Efforts with Health Insurers Cut Medical Claims Errors by Half. 6/18, 2012. <http://www.ama-assn.org/ama/pub/news/news/2012-06-18-national-health-insurer-report-card.page> (accessed 10/24, 2012).
- —. National Health Insurer Report Card. 10/24, 2012. http://www.ama-assn.org/ama/pub/physician-resources/practice-management-center/health-insurer-payer-relations/national-health-insurer-report-card.page?WT.mc_id=NHIRCPR201206&WT.mc_ev=Click (accessed 10/24, 2012).
- NCHAA. Combating Health Care Fraud in a Post-Reform World: Seven Guiding Principles for Policymakers. Whitepaper, Washington, DC: The National Health Care Anti-Fraud Association, 2010.
- NHCAA. The Problem of Health Care Fraud. 10/24, 2012. <http://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-problem-of-health-care-fraud.aspx> (accessed 10/24, 2012).
- Nilsson, Nils J. INTRODUCTION TO MACHINE LEARNING. Stanford, CA: Nils J. Nilsson, 2005.
- U.S. Department of Health & Human Services. “Avoiding Medicare and Medicaid Fraud and Abuse.” [oig.hhs.gov](https://oig.hhs.gov/compliance/physician-education/roadmap_web_version.pdf). 10/24, 2012. https://oig.hhs.gov/compliance/physician-education/roadmap_web_version.pdf (accessed 10/24, 2012).

About the Authors



Shantanu Nigam

Shantanu has spent 14 years of his career in the healthcare compliance industry. A recognized thought leader, he brings a unique mix of deep healthcare domain knowledge, consulting, and delivery credentials. Shantanu spent the majority of his career serving as a leader in Accenture's healthcare practice as a recognized expert in claims authorization processes. He helped multiple healthcare clients going through compliance exercises by building strategy, establishing roadmaps, and driving delivery for many large clients. In addition, Shantanu has held executive leadership positions in other organizations including ACS-Xerox leading large scale mergers and acquisitions and co-founded a pattern recognition company in the late 90's.

Shantanu has been very closely associated and an active participant with various national and international organizations including PAN-IIT, HIMSS, AHIMA, and the Clinical Transformation Group.

To contact Shantanu, please e-mail him at shantanu.nigam@jvion.com.



Surya Vadlamani

Surya comes to Jvion with more than 14 years of leadership experience in the healthcare consulting space. Before Jvion, he spent a majority of his career as a Senior Manager at Accenture in the Health and Life sciences practice. He was responsible for delivery of several transformational and IT initiatives architecting, developing and delivering complex solutions with large teams in the U.S. and offshore for large payor and provider clients. Surya is also Sun Certified Enterprise Architect and possesses unique skills to lead and develop innovative IT solutions. He is the Architect of Jvion's icdcomplete and is responsible for product engineering and client services. Surya is a very active member of the HIMSS and AHIMA organizations.

To contact Surya, please e-mail him at surya@jvion.com.