RiskShield
Turn Risk Into Profit

VOLUME 5
ISSUE 51
AUGUST 2015

Technically Speaking: Fighting Medical Billing Fraud

Tim Rush
INFORM Director of Sales - North America

As insurance experts and subscribers to this newsletter I would believe that you are familiar with terms related to medical billing such as ICD, CPT, HCFA, CMS, EHR, EOB, and the AMD. But what you may not be familiar with is the technology that gives a medical billing or claims fraud detection solution the power to be so successful? When considering the purchase of a software solution, understanding how and why it works can be an important factor in determining its value.

Although fraud detection is becoming one of the top initiatives for carriers today due to its direct impact to their bottom line, I find customers have a level of uncertainty or even doubt regarding its proposed effectiveness. This uncertainty is many times alleviated once there is an understanding of what is behind the curtain that allows it to achieve such measureable results. It's really quite straight forward although vendors often use their own terms to describe it which is not always easy to understand. Let's see if I can help shed some light.

Let's start with the most commonly used technology in the fraud detection product space: ***Predictive Analytics.*** It sounds complicated but really, once explained, the concept is easy to understand.

For a quick definition, 'Predictive analytics applies models to historical data in order to make predictions about future events'.

In a proactive rather than a reactive manner, predictive analytics helps detect new emerging patterns of fraud before they become a payday for a fraudster. In doing so, insurance companies will not only help safeguard their policy holders but also potentially save themselves millions annually in fraud losses.

Predictive analytics, when applied to fraud detection, can detect known patterns of fraud, but can also uncover new and unknown variations based on the data you already have in your claims and policy management systems. In effect, when fraud moves to new areas, suspicious behavior can be detected even if the pattern used by the fraudster is a new strain and has not been seen before.

A key part of predictive analytics, predictive modeling, uses certain approaches or methods to determine future behavior. To stay at a very high level, a typical process in predictive modeling is, data is collected or mined, a statistical model is formulated, predictions are made, and the model is validated (or revised as additional data becomes available). When considering the data for medical

billing fraud, for example, codes could be considered the "raw material" of predictive modeling. Codes define important variables like diagnosis (ICD-9 or 10); procedure (CPT); diagnosis group (DRG – Hospital); drug type/dose/manufacturer (NDC); lab test (LOINC); place of service, type of provider, etc.

A predictive model can use one of several different algorithms or approaches (neural networks, fuzzy logic, genetic algorithms, path finding, natural language processing) that when, combined with some additional capabilities within the predictive models, provide the ability to detect fraud.

As there is no single agreed upon "best" formula, for the purpose of this article, we will focus on two of the most common approaches: 'fuzzy logic' and 'neural network'. Two different methods, but in effect they both can power a fraud detection solution to a similar conclusion.

Fuzzy logic is a form of logic that attempts to deal with reasoning that is approximate, not precise. Instead of dealing with a simple 'true or false' found in other classical forms of logic, fuzzy logic is structured on the 'degree of truth' scenario where the truth value may range anywhere between true and false.

Working with this range instead of an absolute answer allows fuzzy logic to perform reliable decisionmaking where only imprecise data is available, similar to artificial intelligence systems, (Artificial intelligence is the intelligence exhibited by machines or software), however fuzzy logic is usually not regarded as artificial intelligence. Working in conjunction with profiling tools in the model, Fuzzy logic works much the same way our brains work and can recognize a pattern that doesn't look right or a new behavior pattern that it hasn't seen before.

The other approach is the neural network. A neural network is a learning algorithm that is inspired by the structure and functional aspects of biological neural networks. For this explanation, consider a neural network as a system that also thinks and acts like the human brain, learning based on results, recognizing patterns, and making decisions.

A neural network is a machine learning approach that evolved from the study of pattern recognition in artificial intelligence. (Machine learning explores the construction of algorithms that can learn from and make predictions on data). Such algorithms operate by building a model from data inputs in order to make decisions.

To sum up, and I apologize if I offend any engineers who may be reading this, both fuzzy logic and neural networks, when paired with other tools in the model, act similar to the human brain and process data to recognize patterns and make predictions. If you would like to go deeper I can recommend a good text book that is roughly 700 pages specifically on the subject.

There are varying opinions as to which is better, fuzzy logic or neural networks. Scientists and engineers can and do make arguments for both. Each is a different approach that applies their own capabilities to solve the problem at hand: powering fraud detection systems! So, from a technical perspective the two are comparable. I have found however that there are differences, pushing one over the top.

First, fuzzy logic, typically combined in a predictive model with dynamic profiling capabilities, uses its selflearning abilities to decide if the current behavior it is detecting is normal for this customer or not, even if this behavior is subject to change over time. Because of this, a large benefit is achieved where the amount of false positives are reduced (a false positive being an alert detected by the system turning out not to be fraudulent).

The other key difference is that a neural network is typically known as a black box, masking what is inside and how it works, where fuzzy logic is typically transparent, allowing administrators to see all aspects of its operation. This provides clear advantages in the fields of manageability of the model, and response to new fraud MO's and patterns.

So, why is it important to have a predictive analytic based fraud detection system using which ever approach you prefer?

Even if one may approach gets the edge over the other, every insurance company needs some type of detection solution. Conservative estimates tell us insurance companies are spending in excess of $80 billion dollars every year to pay fraudulent claims. The hope is that as vendors continue to educate the marketplace and provide them with a better understanding of the tools available along with the operational benefit, more insurance companies will take advantage of these solutions to fight fraud and therefore improve their bottom line.

In future articles perhaps we can continue to discuss topics that are important in gaining a better understanding of the technical functionality powering today's systems such as pattern recognition, profiling, social network analysis, and many others.

Technology and Medical Fraud

Tami Rockholt, RN
INFORM Director of Business Development, North America

As a nurse who has spent the last 25 years reviewing medical records and bills and fighting fraud, I am amazed by how much technology can speed things up and make experts more effective. When I worked on my very first large scale fraud project in 2003, it took several weeks of analysis to pick out the fraud patterns from the medical billing records. With the advances in technology, a fraud detection program can pick out the same patterns in a fraction of a second. Now the experts and investigators can spend their time taking action, not just looking for fraud.