Predictive Modeling 101: How CMS's Newest Fraud Prevention Tool Works and What It Means for Providers

By Susan E. White, PhD, CHDA

In July the Centers for Medicare and Medicaid Services (CMS) began applying predictive modeling techniques to Medicare claims data to detect fraud. CMS contracted with Northrop Grumman, an information solutions company, to develop the technology. Northrop Grumman partnered with Verizon and National Government Services to develop the platform.[1]

The application of predictive modeling technology to detect Medicare fraud was mandated by the Small Business Jobs Act of 2010, which required CMS implement a program in 10 states by July 1, 2011.[2] However, CMS opted to implement the program nationwide at the outset.

Organizations should understand how CMS's newest fraud prevention tool works and the changes it could bring to claims processing.

What Is Predictive Modeling?

Predictive modeling applies statistical techniques to determine the likelihood of certain events occurring together. Statistical methods are applied to historical data to "learn" the patterns in the data. These patterns are used to create models of what is most likely to occur.

Predictive modeling is used by credit card issuers to determine if transactions are likely fraudulent. Customers who receive a phone call from their credit card company verifying that they authorized a transaction were the subjects of a predictive model.

For example, a customer's typical credit card transaction is $100. The credit card issuer notices that the customer submitted three $5,000 transactions in one day. Given the customer's history and the credit card issuer's historical data regarding fraudulent transactions, those transactions look suspicious.

The credit card company may then put a hold on the card and call to verify that the customer really did authorize the suspect transactions. The triggers that tell the credit card company when to suspect a fraud issue are created via predictive modeling techniques.

Predictive modeling techniques use multiple data sources. Data such as the provider's claim history, the patient's demographics and health status, the services included on the claim, and the attributes associated with previously identified fraudulent claims may all be used to develop a statistical model.

Statistical techniques used to create the model may include logistic regression, cluster analysis, or decision trees. All of these statistical techniques allow the user to combine multivariate historical data into a model that may be used to assess the probability or likelihood that current claims are fraudulent.

In logistical regression, the likelihood that a claim is fraudulent is estimated based on a series of historical data. In cluster analysis, historical data are used to build a model that will measure the "distance" of a claim from the typical claims submitted by that provider or for that type of service. Decision trees use a series of screens or yes/no questions to determine the probability that a claim is valid.

The output of each of these methods is the probability of a claim's validity that is expressed as a score.

The claim score is typically structured so that it is directly related to the probability that a claim is in error. A high score may indicate a high probability that a claim is not legitimate. If the score meets a criteria (either above or below a cutoff value),

then it is identified as a potential error.

The criteria or cutoff value may be used to tune the model to control the sensitivity and specificity of the model. If the cutoff is too extreme, then the model may not be sensitive enough and will allow fraudulent claims to be paid. If the cutoff is not extreme enough, then the model may not be specific enough and identify a large number of false positives.

In the healthcare setting the cost of paying fraudulent claims must be weighed against the cost of withholding payment and reviewing the claim prior to payment. For high-cost/low-volume claims, the cutoff may be set lower to ensure that no questionable claims are paid. The cost of paying an invalid claim outweighs the cost of reviewing a few false positive claims. The model may be adapted and adjusted as more claims history is aggregated.

Scanning for Fraud in Real Time

Prior to the program, CMS used a two-pronged approach to avoid paying fraudulent claims and claims billed in error. On the pre-payment side, claim edits based on coding rules, including the National Correct Coding Initiative edits and medically unlikely edits, are applied prior to payment.

For instance, in the hospital setting the payment logic includes a number of edits that are implemented in the Outpatient Code Editor for the outpatient setting and in the Medicare Code Editor for the inpatient setting. The logic used for these current pre-payment edits are relatively simple "if then" statements and are based only on the content of the submitted claim.

On the post-payment side, CMS utilizes program integrity contractors such as Recovery Audit Contractors to review claims to detect payment errors. Recovery Audit Contractors and other program integrity contractors are currently using a "pay-and-chase" approach. They analyze the paid claims file to detect patterns of data that are unlikely to occur under typical circumstances.

For instance, integrity contractors may request medical records from a provider after observing that a large number of its debridement claims are coded as surgical or that the number of service units provided during a visit is atypical. The data profiling and record requests are performed post-payment.

The provider was paid for the service and now that the contractor observed a potentially incorrect billing, it is the contractor's responsibility to prove the assertion and take back the payment from the provider (the chase).

In contrast, CMS's new fraud detection program attempts to identify potential issues in real time. The claims are screened via a set of predictive modeling rules after being submitted by the provider but prior to payment.

This will likely cause payment delays. In the case of prolonged appeal and litigation, the payment may be withheld for a significant amount of time.

Under the current integrity contractor programs, the provider holds the payment until the issue is settled. The provider runs the risk of owing CMS the incorrect payment plus interest, but the provider has the opportunity to hold onto the payment during the appeal process.

Although CMS has not released any information on the implementation of this new program, it is likely that pre-payment predictive modeling will turn the tables on the provider.

The provider will not receive payment until the identified potential compliance issue is settled. Tuning the predictive model to limit the number of false positives is in the best interest of both CMS and the provider.

For CMS, false positive fraud detection may result in more claims to be scrutinized prior to payment with limited or no return on the review effort. For providers, false positive fraud detection will result in delayed payment and potentially significant administrative efforts to justify the claim as valid.

How Effective Is Predictive Modeling?

Many commercial payers currently use predictive modeling as one of their fraud prevention techniques. The UnitedHealth Group estimated that the use of predictive modeling in the Medicare and Medicaid programs could save the programs $113 billion over the first 10 years of use.[3] A study from the Lewin Group validated the UnitedHealth Group's estimates and further estimated savings of $128.6 billion over the same first 10 years of use.[4]

According to the *Washington Business Journal*, the value of the contract awarded to Northrop Grumman is for $77 million over four years.[5] If the UnitedHealth Group and Lewin estimates are accurate, the return on investment for this program will be significant and positive.

Predictive modeling will be combined with pre-payment edits and the current activities of the payment integrity contractors to provide CMS with a state-of-the-art fraud prevention program.

Notes

1. Centers for Medicare and Medicaid Services. "New Technology to Help Fight Medicare Fraud." 2011. www.cms.gov/apps/media/press/release.asp?Counter=3983.
2. Small Business Jobs Act of 2010. P.L. 111-240 (124 Stat. 2504). http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h5297enr.txt.pdf.
3. UnitedHealth Group Center for Health Reform and Modernization. "Health Care Cost Containment-How Technology Can Cut Red Tape and Simplify Health Care Administration." June 2009. www.unitedhealthgroup.com/hrm/UNH_WorkingPaper2.pdf.
4. The Lewin Group. "Comprehensive Application of Predictive Modeling to Reduce Overpayments in Medicare and Medicaid." July 2009. www.lewin.com/content/publications/PredictiveModelingMedicaidOverpymnt.pdf.
5. "Northrop Grumman Wins CMS Contract." *Washington Business Journal*, June 30, 2011. http://www.bizjournals.com/washington/blog/fedbiz_daily/2011/06/northrop-grumman-wins-cms-contract.html

Susan E. White (susan.white@osumc.edu) is a clinical associate professor in the School of Allied Medical Professions at Ohio State University.

Article citation:
White, Susan E. "Predictive Modeling 101: How CMS's Newest Fraud Prevention Tool Works and What It Means for Providers" *Journal of AHIMA* 82, no.9 (September 2011): 46-47.