“Paying for Care to Dead People”

Boston Herald, October 30, 2011

“Four alleged schemes to defraud MassHealth of $10 million were uncovered after a months long investigation by the Attorney General that found agencies billing taxpayers for care to dead people, widespread kickbacks, or exaggerated claims, prosecutors said.”

FBI News Release, November 15, 2011

ATC, its management company Medlink Professional Management Group Inc., and various owners, managers, doctors, therapists, patient brokers and marketers of ATC, Medlink and ASI, were charged with various health care fraud, kickback, money laundering and other offenses in two indictments unsealed on Feb. 15, 2011. ATC, Medlink and nine of the individual defendants have pleaded guilty or have been convicted at trial. Other defendants are scheduled to begin trial on April 9, 2012, before U.S. District Judge Patricia A. Seitz.

Throughout the course of the ATC conspiracy, millions of dollars in kickbacks were paid in exchange for Medicare beneficiaries who did not qualify for PHP services. The ineligible beneficiaries attended treatment programs that were not legitimate so that ATC and ASI could bill Medicare more than $200 million in medically unnecessary services.
“Real Patients, Real Doctors, Fake Everything Else”

NY Times, October 13, 2010

“By inventing 118 bogus health clinics in 25 states, prosecutors said, a band of Armenian-American gangsters billed Medicare for more than $100 million, and managed to collect $35 million over at least four years. Preet Bharara, the United States attorney in Manhattan, called it the “single largest Medicare fraud ever perpetrated by a single criminal enterprise.”

Eighteen people were charged in the Medicare indictment unsealed on Wednesday, part of a larger ring of 44 people prosecutors said had engaged in a variety of swindles, including bilking auto insurance companies by falsifying, staging or exaggerating the severity of fender-benders. Charges included racketeering, health care fraud, identity theft, money laundering and bank fraud. Forty-one of the defendants had been arrested as of Wednesday afternoon.

“At its heart, the gang, based largely in Los Angeles, resembled a giant identity-theft ring that stole doctors’ dates of birth and Social Security and medical license numbers and paired them up with legitimate Medicare recipients, whose names and information were also stolen. About 3,000 of those patients’ names came from the Orange Regional Medical Center in Middletown, N.Y., the authorities said.”
How Fraud and Abuse Is Located Today
The current state of FWA detection – Limited tool set

- **Claim edits**
  - At the bill level
  - Almost always post-pay – “pay and chase”
  - Limited by “prompt-pay” fears
  - Can create a highly complex web of interactions
  - Processing problem for large payers

- **Rules systems**
  - “Expert system” – open to gaming by experts
  - Also very often at the bill level
  - Also very often applied post-pay
  - High false positives
  - Adding rules is easier than amending or removing

- **Tips and leads**
Opportunities

Eliminate the “Pay and Chase” status quo by looking to other industries, private sector for successful approaches and technologies:

- Identity Proofing/Identity Management – Financial Services, Banking
- Predictive Claims Analytics – Property and Casualty Insurance

Greater focus on the individuals and entities in the program

- Are beneficiaries enrolling who they claim to be?
- Have they disclosed all assets, income, correct state of residence, etc?
- What are the true backgrounds of the practitioners, officers, agents, etc?
- What is the risk profile of a provider based on background, associations, etc.?
- What significant events are occurring between enrollment periods?

CMS Center for Program Integrity (CPI) “National Fraud Prevention Program” focused on prevention and detection that is integrated, risk-based, and measurable; four areas of focus:

- Provider Screening
- Predictive Modeling
- Data Integration
- Case Management
LexisNexis Risk Solutions is a leading global provider of content-enabled workflow solutions to help clients across multiple industries predict, assess, and manage risk.

- Total Revenue: $1.4B (2010)
- Industries Served: Insurance, Background Screening, Financial Services, Receivables Management, Health Care, Legal and Government
- Headquarters: Alpharetta, Georgia
- Number of offices: 34+
- Employees: 4,500

Note: Chart excludes c. $100m law firm revenues included in Legal & Professional
Unique ID

LexisNexis Advanced Linking Technology assigns a unique and persistent identifier to a person

- Dynamic – updates as new public records are available.
- Extremely Accurate - based on multiple public records and data sources
Fraud, waste, and abuse that plagues health care payers can be the result of organized, sometimes collusive, activities among providers and patients.

The identification of large scale rings is important and creates headlines to raise awareness of the problem.

More localized collusion can be harder to find and may be more prevalent.

Using LexisNexis public records database, its High Performance Computing Cluster (HPCC), and advanced data analytics, these collusive relationships can be identified and addressed.

Along with provider of interest identification, this tool allows payers to address fraud, waste, and abuse much more broadly than the traditional bill level approach.
Proactive Fraud Detection: Social Network Analysis

- Connects individuals and entities to create clusters of interest.
- Clusters are augmented with public records information such as assets.
- Advanced analytics finds the most important relationships.
Social Network Analysis Visualization
A top insurer flagged 7 claims as “collusion claims”

Using insurer data alone, a connection between 2 of the 7 claims was found.
Social Network Analysis

Assigned unique IDs to all parties and HPCC added 2 additional degrees of relative data
Collusion in Louisiana AFTER Advanced Linking Technology is Applied

Showed 2 family groups interconnected on the 7 original claims plus linked to 11 more
Predictive Modeling Outcomes

- Tends to be more accurate than other fraud detection methods
- Information collected and cross-referenced from a variety of resources
- Schemes do not depend on up-front assumptions
- Statistically determines key metrics that are associated with claims that have a high fraud-propensity score
Claim Scoring Using Predictive Models

Predictive analytics provides a score for each claim, policy, etc., allowing activity to be concentrated on areas that have the highest probability of financial return.

<table>
<thead>
<tr>
<th>CLAIM NUMBER</th>
<th>SUSPICION SCORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>144618</td>
<td>993</td>
</tr>
<tr>
<td>138514</td>
<td>991</td>
</tr>
<tr>
<td>143949</td>
<td>989</td>
</tr>
<tr>
<td>145594</td>
<td>988</td>
</tr>
<tr>
<td>148531</td>
<td>986</td>
</tr>
<tr>
<td>152506</td>
<td>983</td>
</tr>
<tr>
<td>152787</td>
<td>982</td>
</tr>
<tr>
<td>146937</td>
<td>981</td>
</tr>
<tr>
<td>157651</td>
<td>976</td>
</tr>
<tr>
<td>141970</td>
<td>973</td>
</tr>
<tr>
<td>152271</td>
<td>970</td>
</tr>
<tr>
<td>138703</td>
<td>969</td>
</tr>
<tr>
<td>149491</td>
<td>968</td>
</tr>
<tr>
<td>139439</td>
<td>963</td>
</tr>
<tr>
<td>158952</td>
<td>950</td>
</tr>
<tr>
<td>149319</td>
<td>948</td>
</tr>
<tr>
<td>152602</td>
<td>945</td>
</tr>
</tbody>
</table>

Create the target rich environment.
Provider and Beneficiary Identity Management
<table>
<thead>
<tr>
<th>ENROLLMENT</th>
<th>ASSESSMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISCOVER</td>
<td>DISCOVER: Discover the identity. Undertake data capture, identity resolution and identity enrichment. “Tell us who you are.”</td>
</tr>
<tr>
<td>VERIFY</td>
<td>VERIFY: Verify the identity. Establish that the identity exists. “Does Bob Jones exist?”</td>
</tr>
<tr>
<td>AUTHENTICATE</td>
<td>AUTHENTICATE: Authenticate the identity. Determine whether an individual or business owns the identity. “Are you Bob Jones?”</td>
</tr>
<tr>
<td>EVALUATE</td>
<td>EVALUATE: Evaluate the identity. Assess against legislation, regulations and rules to determine if an individual or business is eligible. “Is Bob Jones eligible?”</td>
</tr>
<tr>
<td>ALERT</td>
<td>ALERT: Alert to identity changes. Receive notification when an individual or business is exhibiting high-risk behavior (continuous evaluation). “Is Bob Jones still eligible?”</td>
</tr>
</tbody>
</table>
Identity Analytics Outcomes: *Beneficiaries*

Reduces beneficiary fraud and ensures accuracy of identity information for program efficiency and risk mitigation

<table>
<thead>
<tr>
<th>Test Criteria</th>
<th>Fraud Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deceased</td>
<td>High</td>
</tr>
<tr>
<td>Identity Fraud Risk</td>
<td>High</td>
</tr>
<tr>
<td>Incarcerated</td>
<td>High</td>
</tr>
<tr>
<td>Occupancy Outside State</td>
<td>High</td>
</tr>
<tr>
<td>Real Property Value and Ownership</td>
<td>Medium</td>
</tr>
<tr>
<td>Motor Vehicle Age and Ownership</td>
<td>Medium</td>
</tr>
<tr>
<td>High Risk Address</td>
<td>Medium</td>
</tr>
</tbody>
</table>

In a recent analysis of a Medicaid beneficiary file:
- over 2% of beneficiaries had a primary address in another state
- 0.59% were deceased
- 2% of adults presented with severe identity fraud risk
Identity Analytics Outcomes: *Providers*

Maintains visibility into provider risk

<table>
<thead>
<tr>
<th>Test Criteria</th>
<th>Fraud Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deceased</td>
<td>High</td>
</tr>
<tr>
<td>HHS OIG Exclusion List</td>
<td>High</td>
</tr>
<tr>
<td>GSA Exclusion List</td>
<td>High</td>
</tr>
<tr>
<td>Felony conviction</td>
<td>High</td>
</tr>
<tr>
<td>State of Licensure, status</td>
<td>Medium</td>
</tr>
<tr>
<td>Known Associates Excluded</td>
<td>Medium</td>
</tr>
</tbody>
</table>

In a recent analysis of a Medicaid provider file:

- Over 1% were deceased
- 1.7% of providers were sanctioned
- A few providers were incarcerated
Program Integrity begins with **knowing** your providers

- Screen all enrolled fee-for-service providers
- Implement robust provider validation and evaluation upon enrollment
- Assign dynamic risk scores and track provider files between enrollment periods for pertinent activity; alerts generated for changes
- Extend enrollment and screening standards to include managed care organizations
Identity Management with public records data as a state priority

- Beneficiary Eligibility systems
- Medicaid Provider enrollment
- Medicaid Program Integrity
- Health Insurance Exchanges
- Health Information Exchanges

Proactive fraud, waste, and abuse detection – social network analysis and predictive modeling - strategies to reducing fraud and increasing cost savings

- Don’t leave it to recovery when there are solutions to stop fraudulent payments before they go out the door
THANK YOU

Kathy Mosbaugh
Director, State Government Health Programs
813.418.2035
Kathy.Mosbaugh@lexisnexis.com