White Paper

The Rise of Organized Crime in Health Care:
Social Network Analytics Uncover Hidden and Complex Fraud Schemes

Experience the power of data, linking and analytics.

December 2011

LexisNexis® | Health Care

Summary

Organized crime has discovered health care in a big way–no surprise given health care expenditures will soon account for close to 25% of GDP. Social network analytics help to unravel organized crime's hidden networks. Increasingly sophisticated and rapidly expanding organized health care fraud threatens both consumers and the sustainability of both government and commercial programs. Law enforcement has ramped up its efforts to pursue the perpetrators, but conventional investigative methods, and even more advanced predictive analytics fraud detection tools, are not enough to successfully address the problem. Social network analysis identifies relationship clusters leveraging "big data" and advanced linking to reveal the relationships that organized criminal networks try so hard to keep hidden, enabling the effective investigation and termination of these insidious and costly rings.

Modernized approach to an old school problem

Organized crime is nothing new. In the U.S., from Prohibition right through the heyday of the old school mafia, organized crime has always sought to get its "share" of every industry where money was being made and not being adequately protected. You want to build something, move something, open a business–we want our share. There were also of course the more traditional pursuits like gambling and drugs. The issue was trying to investigate these crimes. It wasn't long ago when investigators locked themselves away in a "war room" during an investigation with red thread connecting index cards with people's names that were related by blood and white thread connecting those with business relationships.

Not anymore. In an era when "big data" and advanced analytics can be leveraged to discover the matrix of relationships between people, businesses, assets and actions we are no longer locked in the war room forced to slowly unravel the web piece by piece. Using high-powered computing and relational algorithms we can get a clear view of what was only a short time ago not visible.

Organized crime typically conceals itself behind the façade of small businesses, the cover of corporations, or the anonymity of cyber walls. Other industries, such as the financial markets have long dealt with complex criminal structures, including operations that have offshore or international elements. The health care sector lags behind in its efforts to deal with this problem, including employing advanced fraud and abuse solutions.[1]

Social network analytics provide a different kind of data mining, visualized with graphing analysis–a tool that makes significant connections among individuals and behaviors clearer and that correlates relationships between entities that would otherwise go unnoticed.

Migration of organized crime into health care

In Congressional testimony on April 5, 2011, Gerald T. Roy, Deputy Inspector General for Investigations, Office of Inspector General (OIG), U.S. Department of Health & Human Services (HHS), said, "The most challenging and disturbing trend I have witnessed in my tenure . . . is the rise of criminal enterprises in health care fraud."[2] Health care fraud now goes well beyond the cases of individual health care providers, staff, patients or government employees, trying to game the system–the new threats, as pointed out above–are organized, hidden and go from metro to international in scope. The lure of $2.5 trillion dollars and safer, less violent, easier to hide, and less severely penalized crimes is simply too good to resist.

In particular, sophisticated criminal networks are increasingly involved in fraudulent Medicare and Medicaid billing–in part due to the low barriers of entry to these programs that traditionally allowed almost any provider willing to accept the lower reimbursement rates to participate with minimal screening. Although California, New York, and Florida, Texas, and Michigan are traditional hot spots, the cyber nature of these crimes makes them viral and much more likely to spread to anywhere from anywhere.[3]

How they do it

Organized fraud schemes can be relatively straight forward–buy some stolen provider and patient ID numbers, set up a durable medical equipment shop (DME) or other facility, and you're in business. These numbers may be obtained in bulk after being stolen from the trash at hospital, or obtained directly from the providers and patients for a payment of a few hundred each. Schemes can also be quite subtle and sophisticated consisting of a seamless blend of "legitimate" providers and patients, obtaining inflated or unnecessary treatment across a number of insurers: government, commercial and even property and casualty related to staged auto accidents. A ring may pay a few thousand dollars each to a provider or business owner to serve as nominee owner, set up bank accounts, and fill out paperwork. These "legitimate" façades make detection that much harder.

The growing cyber nature of health care facilitates the rapid sale of these billing numbers across the country and helps spread fraud schemes at an alarming rate from ring to ring.[4]

Health care fraudsters bill mostly for primary or specialty clinical visits and for home health care, though community mental health as well as physical and occupational therapy have also become recent targets. Wheelchairs, walkers, and hospital beds are the common foci of medical-equipment scams.[5]

The AARP and HHS have programs to educate the public to spot fraud and scams, to report suspicious activity, and to protect themselves. Consumers need to guard their cards, beware of free services that require a Medicare number, and scrutinize their statements.

Service fraud also includes "ping-ponging" (referring patients to other physicians in the same office), "gang visits" (billing for multiple services or collecting Medicaid recipients and bringing them in groups to clinics for medically unnecessary visits, sometimes paying them or even supplying lunch for such visits), and "steering" (directing patients to particular pharmacies). In some cases the rings have even staged automobile accidents to initiate false medical cases and then billed rehabilitation care, generating millions in total costs to insurance companies.[6]

As is true in general of organized crime in the U.S. and worldwide, health care fraud rings may have strong ethnic ties and have involved criminals of Cuban, Russian, Ukrainian, Asian, Eurasian, Italian, and Middle Eastern background–unfortunately opening concerns as well about a possible nexus between organized crime and terrorism. According to then-Acting Deputy Attorney General Gary G. Grinder, "The emergence of international organized crime in domestic health care fraud schemes signals a dangerous expansion that poses a serious threat to consumers as these syndicates are willing to exploit almost any program, business or individual to earn an illegal profit."[7] Government and private insurers have large intelligence gaps on these networks, even while they base their strategy for dismantling the rings on generating the most robust intelligence possible.[8]

A serious dollar loss: "They're hitting us and hitting us hard," said Timothy Menke, head of investigations for the Office Inspector General (OIG) at Health and Human Services (HHS)[9] whose office estimates that losses for inappropriate government billing for health care services each year at roughly $60 billion, of which the government recovers less than ten percent annually.[10] Estimates place the total loss to health care fraud, from both government and commercial payers at closer to $200 billion.[11] The National Health Care Anti-Fraud Association (NHCAA) calculates that fraud costs the system between $75 billion and $250 billion a year.[12]

Medicare and private insurers pay millions of claims every working day valued at billions of dollars per day. Prompt-pay regulations require them to remit submitted claims within a relatively short period of time, often as little as two weeks, restricting the number of claims that can be reviewed for potential fraud before they are paid. Due to resource limitations, Medicare conducts medical review on less than three percent of all submitted claims before paying them.[13]

Organized criminal healthcare fraud directly escalates the cost and endangers the quality of health care for every American. Real impact on people: health care may be less risky for criminals, but it is clearly the most risky economic crime for patients–it affects every American, not only those who are directly victimized. It escalates the cost and endangers the quality of health care for everyone. Health care fraud and abuse not only contribute to higher insurance premiums, but every dollar paid in fraudulent or abusive claims reduces the amount of money available to improve the quality of care for those incurring legitimate expenses. Medical identity theft often results in fraudsters changing the information on a medical record meaning the next time the victim visits an emergency room they might get the wrong type of blood or be given a drug they are actually allergic to.

"Pill mills" are an important example of how organized crime creates unprecedented risks to consumers. Criminal enterprises posing as pharmacies, often referred to as "pill mills", bilk health care out of millions of dollars by charging payers for massive numbers of fake prescriptions. These phantom pharmacy schemes operate from a real address using a stolen doctor ID along with patient health insurance ID numbers to write fraudulent prescriptions for expensive drugs never actually prescribed or dispensed. Each fake claim can bring in thousands of dollars. A new trend is for more sophisticated organizations to buy legitimate pharmacies, and their owners making detection more difficult. They can then send the money overseas to be laundered.

In June 2010, a doctor and his wife were convicted of running a "pill mill" in a small town in Kansas. Posing as a pain management practice, the clinic run by the couple was open twelve hours a day, seven days a week, and illegally dispensed controlled prescription drugs; meanwhile, they collected more than $4 million from 93 different private insurance and government health care programs. The doctor was found to be responsible for more than 100 overdoses and at least 68 deaths over a six-year period. Among other counts, the doctor and his wife were convicted of health care fraud resulting in death.[14]

Real criminals tend to operate like, well, real criminals. They have threatened investigators and attacked witnesses.[15] They unnecessarily transport patients and subject them to unneeded care that may carry its own risks. They have killed patients. Furthermore, although much of modern healthcare fraud involves the sophisticated manipulation of billing codes and average wholesale price, or off label marketing, the other side of organized crime's aggressive move into our industry is messy and violent. Medical identity theft can prove expensive to its victims–less in direct financial liability than in terms of compromised medical and insurance records that cause problems later. Some Medicare recipients apply for long-term care or other insurance and find they do not qualify because their medical records include fraudulent treatments and tests. In addition, when scams get particularly popular, Medicare cracks down on eligibility, making it more difficult for those who truly need the help.[16]

What the government has done so far

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) set up a national Health Care Fraud and Abuse Control (HCFAC) program under the direction of the OIG and HHS to coordinate federal, state, and local law-enforcement activities, and in 2010 the federal government spent an unprecedented $1.7 billion to combat fraud, waste and abuse.[17]

Although there is no "three-strike" rule or death penalty for health care fraud, changes in the Federal Sentencing guidelines are making penalties far more severe and costly to the perpetrators, particularly the C-Suite. Penalties for charges recently have included, in addition to repayment, a $500,000 fine and life in prison. Specific changes include:

- A two-level increase in the offense level for any defendant convicted of a Federal health care offense relating to a Government health care program which involves a loss of $1 million to $7 million;
- A three-level increase for losses of $7 million to $20 million; and
- A four-level increase for losses of more than $20 million.

Graphing analysis displays degrees of association and confidence for each relationship linkage shown. Variables computed can include personal information as well as data on businesses, assets, and properties.

In addition, language in the federal health care reform bill made changes to the False Claims Act:

- Any overpayment identified by a provider and not reported and refunded is a violation of the FCA. Identified overpayments must be reported and refunded within 60 days of being identified or within 60 days of the date an corresponding cost report is due
- Civil monetary penalties for each FCA offense increased from $5,500-$11,000 per claim to $50,000 per claim
- Violators are subject to treble damages–can be fined up to three times the $50,000 per occurrence

James G. Sheehan, a former Federal Prosecutor and former Medicaid Inspector General of New York, has taken a progressive and enterprise wide approach to reducing health care fraud. Moving from his former work in simply prosecuting these crimes, his work in New York resulted in the recovery of more than $1.2 billion in improper Medicaid payments in four years starting in 2006 and helped his state's Medicaid program avoid paying $2 billion more. His agency has excluded nearly 4,900 providers and cut off an additional 1,763–more than any other state. Sheehan pioneered an approach that emphasized working with providers to uncover vulnerabilities, publishing a work plan to notify providers of areas of focus and aggressively enforcing laws for those who ignored the warnings.[18]

Swimming with the sharks–using the remora to identify the sharks

Both government and commercial payers are beginning to understand how multi-dimensional fraud controls can be leveraged to get at the roots of organized fraud. These approaches address workflow (pre-pay), manpower (enterprise wide involvement) and analytics (predictive modeling and social network analytics). The government's primary tool for shifting from a case by case approach to a more network driven approach to attacking fraud are the Healthcare Fraud and Prevention and Enforcement Action Teams (HEATs). HEAT Strike Forces leverage access to a wide range of tools and resources, and, most importantly, signify a sustained focus and support by senior level leadership. In geographic areas at high risk for Medicare fraud, the Strike Forces pursue a technologically sophisticated and collaborative approach. Instead of relying primarily on insiders with knowledge of schemes, though, Strike Force cases are data driven, using technology to pinpoint fraud hot spots, starting with identifying inexplicable billing patterns as they occur.

"Much of our attention has been focused on obtaining real-time data," says Menke about the HEAT initiative, adding that additional "real-time data access would enable us to more efficiently conduct field surveillance, electronic monitoring, and issue search and arrest warrants." In Congressional testimony, he adds that the more current the data, the more effective agents can be in:

- Confronting a witness who may be lying or withholding information;
- Identifying relevant parties, locations, and times to conduct surveillance or electronic monitoring operations in order to have the best chance to observe an ongoing criminal operation;
- Planning a search warrant to quickly and accurately locate evidence of a crime before perpetrators destroy, alter, or manufacture information; and
- Planning an arrest warrant to quickly determine the location of a subject before the subject is alerted to the investigation and has an opportunity to flee or prepare for law enforcement arrival if the subject does not intent to cooperate.[19]

The Next Step: Leveraging big data and analytics to make hidden collusion visible

One thing is clear–traditional methods alone are not adequate
Leaders and decision makers need to question whether the tools they have allocated to combat organized crime are still effective for countering today's risks. Despite the best efforts of domestic and international working groups and task forces, fraud by organized crime remains a massive and growing problem. Conventional efforts to stop such crime, while yielding more recoveries each year, simply are not enough and are recapturing only a small percentage of the losses. Experts estimate that a more preventive, proactive model could net Medicare alone as much as $70 billion a year in savings,[20] potentially providing a major opportunity to slow spiraling health care spending as a percent of GDP.

New provider enrollment rules under the Affordable Care Act (CMS Rule 6028) seek to ensure that providers and suppliers are screened for their risk of committing fraud, waste, and abuse before being allowed to enroll in federal programs. For now though, payers accept and pay the vast majority of claims without sufficient analytics to determine their legitimacy–there is very little prepayment scrutiny beyond simple business rule edits. Likewise, post payment cases are investigated and recovery chased down on a case by case basis with very little insight as to the root cause of the cases.

Legislative efforts to fight health care fraud continue and could require CMS to apply a comprehensive pre-payment predictive process to all claims.[21, 22] Predictive modeling techniques can accomplish this by:

- Using statistical analysis to discover previously unknown fraud schemes linked to unidentified metrics;
- Collecting and cross-referencing information from a variety of sources, providing a better balance of data than the more labor-intensive, rules-based system; and
- Replacing up-front assumptions associated with a rules-based approach with a data mining and predictive modeling process that statistically determines key metrics that are associated with claims that have a high propensity for fraud.

As vital a tool as predictive modeling is, however, it does not have the ability to identify connections or relationships between various players within a health care fraud scheme. This is the value of social network analytics.

Large-scale graph analytics, generally thought to be the domain of companies like Google, now see expanded use for exposing unseen patterns:

- Twitter®, Facebook®, LinkedIn® and other social-network platforms use graph analysis-type paradigms to determine who's connected to whom in the cybersphere.
- Google™ uses graph analysis to power its page-rank and ad-targeting features.
- LexisNexis® uses graph analysis to resolve identities and combat fraud.

What social network analytics does—making the hidden visible

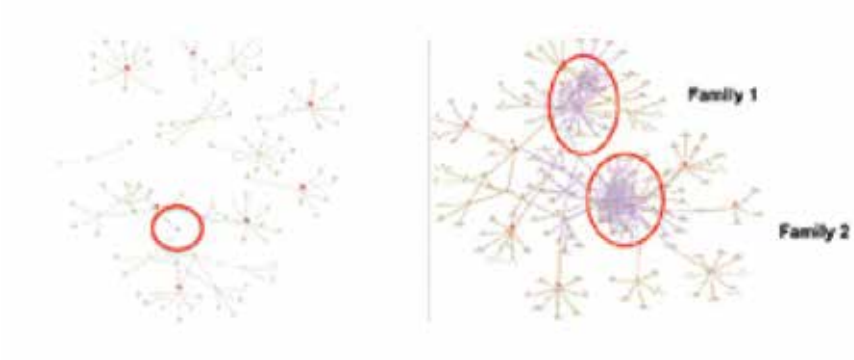
New social network analytics help identify relationships and interactions within clusters of individuals, including:

- Patient relationships with known perpetrators of health care fraud;
- Links between recipients, businesses, and assets, as well as relatives and associates;
- Links between licensed and non-licensed and sanctioned providers; and
- Inappropriate relationships of employees, suppliers, and partners with patients and providers.

Using massive data sets, powerful computing and advanced association algorithms, Social Network Analytics (SNA) reveal organized activity, even when those engaged in it are trying to stay hidden. Leveraging vast public records databases that go well beyond phone and address and other "credit header" type information, SNA reveals connections between entities, assets, and people that would otherwise remain hidden. Social network analytics can thus focus in to reveal the roots and tentacles of fraud within a provider network.[23]

LexisNexis® analytics consider thousands of attributes to identify data patterns that can be used as indicators of the level of risk associated with a particular provider. The information analyzed includes more than 34 billion proprietary and non-proprietary public records, approximately 50 terabytes, constantly refreshed, that can be linked with client data.[24] The industry's most powerful internal data-linking analysis and technology relies on a massive parallel-processing open-source computing platform (the High Performance Computer Cluster http://hpccsystems.com/). [25]

Social network analytics use algorithms that aggregate linkages into high-value clusters of interest, illustrated by graph analysis (see figures). Maps of transportation systems or disease epidemics, or of connections that the web itself makes among subject matter, are examples of graph analyses. Graph analysis built on relationships ingests and integrates massive volumes of disparate data to determine who and what go together.



Adding other dimensions to enhance resolution. Using its own internal data and traditional linking methods, a private insurer found just one link between seven insurance fraud schemes, representing hundreds of suspect medical claims. By employing advanced social network analytics, LexisNexis linked the insurer's internal data to the a public-records database and identified 11 additional potential fraudulent schemes directly related to the original seven, as well as two families that appeared to be at the center of the activity.

In pursing healthcare-fraud criminals, LexisNexis social network analytics can look at clusters of the most significant statistics for that particular case and, for example, additionally query how many beneficiaries, or other individuals they are linked to, are, for example, living in expensive residences, own expensive property, drive expensive cars, or are contacts of medical businesses, further combining these variables with connections to providers, benefit details, dollar amounts, and treatment history.

What social network analytics produce

The Omnibus Crime Control and Safe Streets Act of 1968 granted law enforcement the ability to wiretap suspects and their associates, revolutionizing the pursuit of organized crime. Social network analytics offers a 21st Century version of this paradigm shift.

Wire taps and surveillance can be tremendous tools for building a case once you have already figured out who you want to investigate. By linking and analyzing virtually unlimited quantities of data, social network analytics can expose hidden collusion and reveal networks long before a traditional investigation would even be an option. By leveraging the analysis of both internal and external data, this approach allows payers and prosecutors for the first time to stay one step ahead of perpetrators by asking: What behaviors are predictive of fraud? This powerful tool exposes ringleaders and brokers who may not be members or beneficiaries, and therefore lie outside of the payer's data. Without social network analytics these links are virtually impossible to discover unless you rely on luck or tips.

Consider the value of knowing that what you thought was a localized health care fraud scheme involving one family was actually a multi-state crime ring involving multiple families and not just one type of criminal activity, but several, costing you ten times what you thought it was across your coverage area. Or, imagine how challenging it would be to investigate several hundred Medicaid recipients discovered to be living in the same high-end beach front condominium complex but with no obvious connection to one another other than all being of one ethnic background. The number of man-hours required to investigate these individuals and the volume of information to be reviewed using traditional investigation methods is overwhelming, to the point of simply being impossible. Social network analytics can do that same work in a matter of hours, uncovering levels of relationships that might never have been discovered using a manual process.

Most importantly imagine each month being delivered organized, visualized, reporting consisting of high value clusters of interest that you had no idea existed. Each cluster representing the potential for cost savings and recoveries.

Law enforcement agencies and health insurers have witnessed the migration of criminals away from drug trafficking and more violent and heavily penalized areas of crime into the safer and more lucrative business of health care fraud. While health care fraud will never be completely eradicated, rapid advancements in technology are allowing insurers to use a larger variety of powerful techniques to prevent and detect it. Fully automated social network analytic tools that identify potential collusion across an entire book of business, uncovering in seconds relationships that previously took months or years to find, or simply remained hidden forever, will make it increasingly difficult for organized crime to hide behind the complexity of their operations. The more difficult it becomes for them to conduct their schemes without detection–and the more difficult early detection makes it for them to replicate those schemes elsewhere–the less attractive health care fraud will be for organized crime, and the more dollars will be saved by your organization.

Healthcare fraud costs money. Organized crime likes money. Social network analytics, for the first time, enables us to see the full scope of fraud and abuse and thus take proactive steps to prevent organized fraud rings from settling in and systematically drawing vital resources from an already strapped system. We must reduce the overall cost of health care without negatively impacting legitimate providers to ensure the solvency of both government and commercial payers. Only then can our health care dollars be spent delivering quality care in the right setting at the right time to every individual.

Sources

[1] Enterprise Fraud and Misuse Management Solutions: 2010 Critical Capabilities, 29 October 2010, Gartner, Inc.
[2] Congressional Documents and Publications, April 5, 2011, Federal Information and News Dispatch, Inc
[3] The Department of Health and Human Services and The Department of Justice, Health Care Fraud and Abuse Control Program, Annual Report for Fiscal Year 2010, January 2011
[4] A Perspective on Fraud, Waste, and Abuse Within The Medicare and Medicaid Programs, Testimony of Gerald T. Roy, Deputy Inspector General for Investigations, Office of Inspector General, U.S. Department of Health & Human Services
[5] Congressional Quarterly HealthBeat, March 2, 2011 Medicare Fraud Going 'Up, and Up, and Up,' Republicans Charge
[6] The Globe and Mail (Canada), December 27, 2010 Bumper To Bumper Fraud; Grant Robertson And Tara Perkins Examine Staged Accident Rings, The Collusion Of Some Health-Care Clinics And The Huge Payments Drivers Are Bearing To Absorb The Growing Costs Of Criminality That Insurers And Regulators Seem Unable To Stop
[7] NewsWithViews.com, November 6, 2010 Organized Crime's Involvement in Government Health Care. Jim Kouri, CPP. http://www.newswithviews.com/Kouri/jim120.htm
[8] Strategy to Combat International Organized Crime, U.S. Department of Justice, April 2008
[9] October 22, 2009, By Allan Chernoff and Sheila Steffen, CNN.com, http://articles.cnn.com/2009-10-22/justice/medicare.organized.crime_1_organized-crime-medicare-patients-medicare-and-medicaid?_s=PM:CRIME
[10] Investigation of Health Care Fraud, U.S. Department of Health and Human Services, Office of Inspector General
[11] October 2009 Thomson Reuters Report http://www.reuters.com/article/2009/10/26/us-usa-healthcare-waste-idUS TRE59P0L320091026
[12] Managed Healthcare Executive, April 2011, Insurers Want MLR Policies To Include Anti-Fraud Efforts
[13] PROGRAM INTEGRITY, August 24, 2010 Bob Foster, CMS Atlanta
[14] Combating Health Care Fraud in a Post-Reform World: Seven Guiding Principles for Policymakers. NHCAA White Paper. October 6, 2010. P5.
[15] CBS News, October 7, 2009 Health Care Goodfellas: Mafia turns to Medicare Fraud http://www.cbsnews.com/8301-504083_162-5368496-504083.html
[16] The New York Times, October 30, 2010, Be Alert to Protect Yourself Against Medicare Fraud
[17] The Supercharged Federal Effort to Crack Down on Fraud and Abuse Health Affairs, 29, no.6 (2010): 1093-1095
[18] Philadelphia Inquirer, 8/31/11
[19] Testimony before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, March 4, 2010, Testimony of: Timothy J. Menke, Deputy Inspector General for Investigations Office of Inspector General, U.S. Department of Health & Human Services
[19] Philadelphia Inquirer, 8/31/11
[20] http://www.thefiscaltimes.com/Articles/2011/03/10/Medicare-Fraud-A-70-Billion-Taxpayer-RIpoff.aspx
[21] Grassley Fights Fraud in Medicare and Medicaid, March 2, 2011, Sen. Chuck Grassley (R-IA) News Release Federal Information and News Dispatch, Inc.
[22] Congressional Documents and Publications June 15, 2010, House Ways and Means Subcommittee on Health Hearing; Hearing on Reducing Fraud, Waste and Abuse in Medicare; Testimony by Rep. Roskam, Peter J. - (R-IL), Federal Information and News Dispatch, Inc.
[23] Bending the Cost Curve: Analytic Driven Enterprise Fraud Control, LexisNexis white paper, 2011
[24] LexisNexis® Social Network Analytics for Health Care, 2011
[25] Presentation, World Health Care Congress, Bill Fox, JD, MA, Senior Director Health Care, LexisNexis Risk Solutions

For More Information:

Call 800.869.0751 or visit www.lexisnexis.com/risk/healthcare

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government assess, predict and manage risk. Combining cutting-edge technology, unique data and advanced analytics, LexisNexis Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a world leading provider of professional information solutions.

Our identity management solutions assist states with ensuring appropriate access to public benefits, enhance program integrity and operational efficiency, reduce the impact of identity theft and fraud, and proactively combat fraud, waste and abuse throughout government programs. Our health care solutions assist payers, providers, and integrators with ensuring appropriate access to health care data and programs, enhancing disease management contact ratios, improving operational processes, and proactively combating fraud, waste and abuse across the continuum. The NAC is in the unique position to benefit by overlaying state data with the complex analytics of LexisNexis's solutions.

LexisNexis® | Health Care