LexisNexis® RISK SOLUTIONS | Health Care

NHCAA National Health Care Anti-Fraud Association®

WHITE PAPER

Enhanced data for more powerful fraud prevention

New research demonstrates the value of enhancing SIRIS with data from external sources to boost provider fraud detection and prevention.

NOVEMBER 2016

ENHANCED DATA FOR MORE POWERFUL FRAUD PREVENTION

Health care reforms, and more specifically, performance-based payment models, have placed pressure on providers to adapt to completely new business models. Many providers are finding it difficult to stave off profit decreases. Unfortunately, this added financial pressure has seemingly motivated an increased number of providers to choose fraud, waste or abuse as a tactic for subsidizing their shrinking bottom lines.

Health care fraud and error losses were $487 billion in 2011. Reductions in fraud and error losses of up to 40% are possible within one year—freeing up to $195 billion.[1]

NHCAA members fighting fraud together

One tactical response to the increases in provider fraud has been collaboration among members of the National Health Care Anti-Fraud Association (NHCAA) to develop and implement the Special Investigation Resource and Intelligence System (SIRIS). Designed and powered by LexisNexis® Risk Solutions, SIRIS is a contributory database that allows NHCAA members to submit, track, monitor and share information related to potential provider fraud and associated investigations. While SIRIS is a valuable tool for information sharing and screening providers for previous suspicious activity, its fraud detection capabilities can be augmented by combining external derogatory data.

What if we infused SIRIS with LexisNexis data?

In the fall of 2016, LexisNexis and the NHCAA partnered to conduct a research study to assess the value of adding external provider derogatory data to SIRIS.

RESEARCH STUDY METHODOLOGY	RESEARCH STUDY OBJECTIVE	RESEARCH STUDY CONCLUSION
Researchers analyzed more than 8,000 SIRIS providers using LexisNexis data and analytics to determine if any derogatory information was returned	Determine if a meaningful correlation exists between the derogatory flags found within LexisNexis data and suspicious provider data found in SIRIS	Derogatory factors showing a high percentage of correlation with providers in SIRIS suggest that those factors are strong indicators of potential fraudulent activity

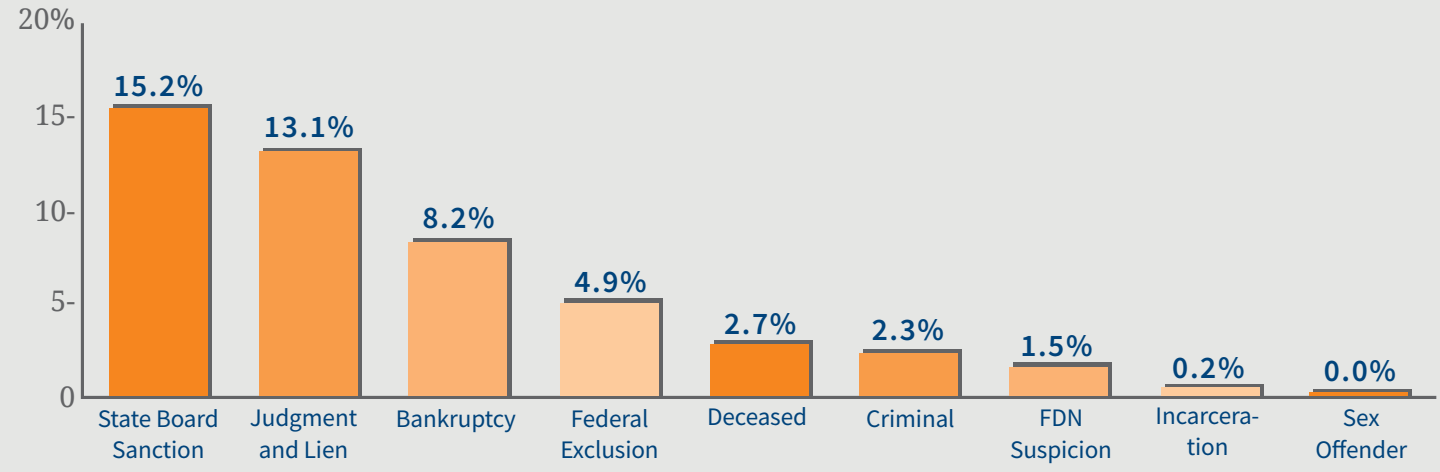
More data input—more insightful output

Overlaying various types of LexisNexis data onto the SIRIS database provided a multi-dimensional perspective of providers, which is unavailable in the SIRIS database alone. The additional layers of LexisNexis data applied in the study included:

HEALTH CARE DATA	NON-HEALTH CARE INDICATORS	FRAUD INQUIRIES FROM OTHER INDUSTRIES THROUGH THE LEXISNEXIS® FRAUD DEFENSE NETWORK
Exclusions, Licenses, Sanctions, NPI & DEA	Criminal, Sex Offender, Deceased, Bankruptcy, Liens & Judgments	Financial Services, Insurance & Government

The LexisNexis® Fraud Defense Network (FDN) connects professionals and organizations across industries with best practices, resources and innovative fraud prevention tools to better attack fraud. An important part of this initiative is a data repository that houses information about fraudulent and suspicious events gathered from organizations in finance, health care, insurance, communications, government and other industries. The database alerts contributing organizations to broad-based activity that may be indicative of higher-than-average risk potential for fraud. In short, FDN assists in connecting the dots between different industries to further improve the fraud mitigation and prevention efforts.

Percentage of SIRIS providers that matched some provider derogatory elements:



Number of providers:	1,274	1,098	689	409	228	192	124	20	1

INSIGHT #1

Incorporation of external derogatory provider data can expose providers that possess strong indicators of fraud:

- Bankruptcy, liens and judgments may be motivating factors for providers to commit fraud—and may be underutilized for predicting and monitoring possible fraud before it happens.
- Medical license expirations, current sanctions and exclusion lists and deceased providers should continue to be reviewed by payers.
- Criminal records did not appear to be a direct indicator of fraud in this study, but have been proven to show relationships of fraud in other studies. As an example, providers who have prior criminal convictions in a different locale and/or relationships to convicted criminals and related businesses have been proven to commit fraud again in the future and are worth monitoring.

INSIGHT #2

Using the LexisNexis Fraud Defense Network to leverage fraud inquiries and confirmed cases across multiple industries:

- Provides signals that are highly predictive of fraud
- Can often provide signals of potential fraud earlier than monitoring inquiries within just the health care market

Promising results

EXAMPLE #1:

The study revealed multiple examples of bankruptcies filed in the year before SIRIS conducted investigations for phantom services and upcoding issues.

EXAMPLE #2:

A large lien and judgment amount was imposed on a provider prior to SIRIS investigations for services not provided and repeated instances of upcoding.

EXAMPLE #3:

The LexisNexis Fraud Defense Network has **detected 124 SIRIS providers** at high risk for fraud from outside of health care, including:

- One provider investigated for financial services fraud three times and insurance fraud one time the year before being added to SIRIS
- Another provider investigated for fraud related to legal services once and debt collection once—both during the year prior to being added to SIRIS

Summary

Leveraging certain types of data, like licensing expirations and deceased records, allows insurers to withhold payment for further investigation of fraud. Other types of data, like bankruptcies or past fraud inquiries within other industries, help insurers to identify indicators of potential fraud. The ability to predict the likelihood that a provider has committed or may commit fraud in the future enables insurers to prioritize providers based on risk and optimize resource allocation for monitoring, investigating and preventing fraud, waste and abuse. Is your health plan leveraging this powerful external derogatory and cross-industry data to improve your SIU's performance?

Sources:

[1] BDO International, March 2014, http://www.insurancefraud.org/statistics.htm#13

For more information, call 866.396.7703 or visit
lexisnexis.com/risk/health-care

LexisNexis® RISK SOLUTIONS | Health Care

NHCAA National Health Care Anti-Fraud Association®

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 predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide 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 RELX Group, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our health care solutions combine proprietary analytics, science and technology with the industry's leading sources of provider, member, claims and public records information to improve cost savings, health outcomes, data quality, compliance and exposure to fraud, waste and abuse.

NXR11577-00-1116-EN-US