In April 2016, the Iowa Medicaid Enterprise (IME), part of the Iowa Department of Human Services, launched Iowa Health Link—a managed care program that offers Medicaid members access to physical, behavioral and long-term care benefits from a managed care organization (MCO) of their choosing. The state was still responsible for fighting fraud, waste and abuse in its Medicaid program, but under managed care, the task became more complex. In addition to surveilling traditional provider payments made from the state or MCO directly to providers, managed care added the complexity of a second payment—the capitation payments made to MCOs.

**Overview**

**The need**
Iowa Medicaid Enterprise (IME) needed help fighting fraud, waste and abuse in its new managed care program.

**The solution**
IME utilized the flexible analytic capabilities of IBM DataProbe® to run specialized algorithms that mined for the highest priority vulnerabilities.

**The benefit**
After analyzing more than $15 billion in Medicaid dollars paid to providers, IME recovered over $22.3M during the State Fiscal Year 2018 over a 12-month period.

**Iowa Medicaid Enterprise**

State Medicaid program uses DataProbe to recover millions of dollars in fraudulent and wasteful claims.

In April 2016, the Iowa Medicaid Enterprise (IME), part of the Iowa Department of Human Services, launched Iowa Health Link—a managed care program that offers Medicaid members access to physical, behavioral and long-term care benefits from a managed care organization (MCO) of their choosing.
also had to be reviewed. In addition, under- and over-utilization had to be monitored to ensure that MCOs were not denying or restricting medically necessary treatment.

**Strengthening program integrity with robust analytics**

IME turned to the program integrity (PI) team at IBM Watson Health™, for help detecting, deterring and recovering Medicaid fraud, waste and abuse in its new managed care program.

Using IBM DataProbe, the team built a PI database by integrating and standardizing six years of fee-for-service and managed care data history, including claims (paid and denied), eligibility, provider files and several reference files. Then, they created a library of custom predictive analytics to identify complex schemes as well as simple billing mistakes. They used both parametric and non-parametric methods for anomaly detection, which included clustering techniques to identify peer groups with normal claims behaviors whose homogeneity has been enhanced not only by specialty designation, but also practice setting, procedure mix fingerprints, geography and other relevant data-driven factors. The results were presented as straightforward alerts as well as multi-variate composite scoring, supporting risk-stratified provider scorecards. This approach provided high-quality leads with fewer false positives than less-structured predictive models.

**Getting results—and accolades**

The Watson Health PI team helped IME analyze more than $15 billion in Medicaid dollars paid to providers. Several high-priority targets were identified, and a series of desk and field-based audits and investigations were launched. As a result, over $19.2 million was recovered during a 12-month period.

$19.2M recovered during 12-month period

$15B Medicaid dollars paid to providers

Due to the innovative use of DataProbe and impressive performance improvement results, IME was honored with a 2017 Truven Health Advantage Award in the category of Strategy and Growth.

The team also created a comprehensive framework to provide oversight to Special Investigations Units for each of the MCOs operating in Iowa. And, in a recent review of the state’s Medicaid program, CMS commended IME for its ability to detect and mitigate risks associated with provider enrollment and ongoing verification checks.
About IBM Watson Health

Each day, professionals throughout the health ecosystem make powerful progress toward a healthier future. At IBM Watson Health, we help them remove obstacles, optimize efforts and reveal new insights to support the people they serve. Working across the landscape, from payers and providers to governments and life sciences, we bring together deep health expertise; proven innovation; and the power of artificial intelligence to enable our customers to uncover, connect and act — as they work to solve health challenges for people everywhere.

For more information


Solution component

IBM® DataProbe®

Connect with us

© Copyright IBM Corporation 2019

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2019

IBM, the IBM logo, ibm.com and Watson Health are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at [ibm.com/legal/copytrade.shtml](ibm.com/legal/copytrade.shtml).

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The information in this document is provided “as is” without any warranty, express or implied, including without any warranties of merchantability, fitness for a particular purpose and any warranty or condition of non-infringement.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others.

No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.